FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Análisis jurídico de la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTORES:

Quispe Ayala, Victor Faustino (orcid.org/0000-0003-0407-5723)

Quispe Saire, Laura Sofia (orcid.org/0000-0002-6868-8839)

ASESOR:

Dr. Chavez Suarez, Giancarlo Renan (orcid.org/0000-0001-8053-6136)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de Penas, Causas y Formas del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA - PERÚ

2023

Dedicatoria

A dios que me dio la fortaleza, para llegar a la meta
A mis hijos por su paciencia y comprensión y amor.
Permitieron cumplir mi sueño.
Att: Víctor Quispe
A mi familia, pero en especial a mis hermanos.
A mis padres que me apoyan para que pueda cumplir mis metas
Att: Laura Quispe

Agradecimiento

A dios por darnos fuerzas para poder continuar con el trabajo de investigación, a los docentes, por tener paciencia y brindarnos el apoyo necesario para lograr terminar el trabajo de investigación.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

La presente investigación surge al evidenciar los problemas que existe en el delito de suplantación de identidad por la falta de la regulación de la Ley N° 30096, mediante transacciones comerciales compra y venta por internet; tiene como problema general ¿Cómo se manifiesta la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos? Asimismo, como objetivo general, fue Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios digitales.

Por otro lado, la metodología utilizada fue el enfoque cualitativo, de tipo básica, con un diseño exploratorio y de diseño específico análisis documental, se formulara estrategia para alcanzar los resultados en la investigación. La población y muestra a utilizarse, fueron 10 abogados y revisión sistemática de la literatura, que cumplieron con los criterios de inclusión.

Para la obtención de información como instrumentos se aplicó, la guía de entrevista a profundidad y la guía de revisión documental, aplicando la sistematización de datos la técnica de análisis de contenido. Finalmente, se llegó a la conclusión que por falta de la regulación de la Ley 30096 ,las transacciones comerciales de compra y venta por internet son una fuente para que desconocidos vulneren la información personal utilizando técnicas como el phishing y el vishing siendo estas las más usuales.

Palabras Claves: suplantación de identidad**,** phishing, vishing, virus informático

Abstract

The present investigation arises by evidencing the problems that exist in the crime of identity theft due to the lack of regulation of Law No. 30096, through commercial transactions of purchase and sale over the Internet; It has as a general problem, how is the ineffectiveness of Law No. 30096 manifested in the crime of identity theft by computer means? Likewise, as a general objective, it was to determine the way in which the ineffectiveness of Law No. 30096 affects the crime of identity theft through digital media.

On the other hand, the methodology used was the qualitative approach, of a basic type, with an exploratory design and a specific documentary analysis strategies will lead as a strategy to achieve the results in the investigation. The population and sample to be used were 10 lawyers and a systematic review of the literature, who met the inclusion criteria.

To obtain information, the in-depth interview guide and the documentary review guide were applied as instruments, applying the data systematization of the content analysis technique. Finally, it was concluded that due to the lack of regulation of Law 30096, commercial purchase and sale transactions over the Internet are a source for strangers to violate personal information using techniques such as phishing and vishing, these being the most common.

Keywords: identity theft, phishing, vishing, computer virus, identity theft.

I. INTRODUCCIÓN

La pandemia originado por la covid-19, en el mundo y el Perú, se determinó que el gobierno peruano decretara el estado de emergencia sanitaria en todo el país, para evitar el contagio de los trabajadores, se implementó el trabajo remoto utilizando la tecnología informática, para que las empresas e instituciones del Estado continúen desarrollando actividades, los trabajadores realizaban sus funciones desde su casa en forma virtual, por tal razón se incrementó en forma acelerada el uso de los equipos tecnológicos, tales como computadoras de mesa, laptops, tables y celulares.

Así mismo, indica Chigirev (2021) Es fundamental señalar que el aumento de las personas que realizan teletrabajo fue creciendo sistemáticamente en los últimos años, Eurostat (2018), por otro lado, la crisis sanitaria ha generado la adopción, por parte de los empleadores, la modalidad de trabajo remoto. Teniendo este el entorno como el de la pandemia del COVID-19 el trabajo remoto ha demostrado ser una estrategia importante para garantizar la resiliencia operativa de los organismos públicos y privados.

En ese mismo orden de ideas, las personas no asistían en forma presencial a efectuar transacciones comerciales, por tal razón se incrementó la banca móvil, los pagos por internet, compra y venta vía online, giros de dinero también virtual, esto ocasiono que delincuentes, realicen delitos informáticos de suplantación de identidad, clonación de tarjetas, para realizar los siguientes ilícitos: transferencia de dinero vía online, compra por tarjetas de crédito o débito, los delitos informáticos se incrementaron en forma alarmante en especial la suplantación de identidad digital, lo cual es materia de análisis del presente trabajo de investigación.

Martínez (2018) La tecnología ha contribuido a desarrollar lo “económico, social y político”, desarrollando también las potencialidades de las personas, al mismo tiempo se ha incrementado las conductas inapropiadas y perniciosas contra terceras personas, lo que denomina “delitos informáticos”, en muchos casos a nivel mundial.

Martínez (2018) se configura el fraude informático el que vulnera contra el patrimonio de terceras personas, “igual que todas las causas de estafa, tiene que configurar el provocar un perjuicio, de sus bienes a otra persona”. Considerado como el bien jurídico protegido castigando el proceder que afecta el patrimonio, a través del uso de medios informáticos por parte del ciberdelincuente.

Temperine (2018) El avance que ha presentado la ciberdelincuencia durante los últimos años, sobre todo las organizaciones criminales (cibercrimen) señalados en este tipo de delitos. En otras palabras, el ciberdelito como negocio demanda un incremento en los accesos para que sea redituable. Son efectuados sistemáticamente en todas partes del mundo (transaccionalidad del delito), por ello, la automatización del atentado virtual, incentiva el desarrollo de herramientas legales que castiguen estos delitos.

En ese orden de ideas Ofaec (2021) la Ciberdelincuencia se entiende en sentido riguroso, como el comportamiento ilícito verificado con operaciones digitales que vulnera y arremete contra la seguridad de los sistemas informáticos y datos que se procesan. También (Sain,2018), Desde el punto de criminológico existe dos enfoques, el primer delito informático son habituales que se forman a partir de mecanismos electrónicos y el uso de internet. La segunda se manifiesta por el huso de la tecnología de la información y comunicación.

Con respecto a la suplantación de identidad El artículo 9.de la Ley N°30096, señala: El que, mediante las tecnologías de la información o de la comunicación, suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. Aquí podemos notar que existe vacíos sobre los delitos informáticos, debería especificar sobre la transferencia financiera, que realizan los ciberdelincuentes después de obtener toda la información de tus datos personales, para luego realizar la suplantación de identidad y cometer delitos, considerando a los datos digitales personales como un bien jurídico que debe ser protegido.

Como indica el Código Penal, Art.207-B (2004) el que utiliza o obstaculiza indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte del sistema con el fin de alterarlo, dañarlos o aniquilarlos, se le impondrá una pena privativa de la libertad no menor de tres ni mayor de cinco años

y con setenta a noventa días multa.

No específica sobre los datos digitales personales que son utilizados, para realizar la suplantación de identidad.

Por ello sobre delitos informáticos, Lucerna (2021) manifiesta el ejemplar clásico de autoridad y dominio de la información ha tomado un nuevo punto de vista, el ejemplar actual se manifiesta en el control de la información tal como se evidencio en diversos sucesos de connotación internacional, por ejemplo, el caso de los WikiLeaks, evidenciándose, al día de hoy, con influencia a diversos países y personas que han logrado resaltar significativo crecimientos en el marco tecnológico.

Cavada (2020), concluye que el término “cibercrimen” presenta una escasez de definición universalmente homogénea y verificada por los expertos en el área, evidenciando un pacto entre los examinadores en que sería una actividad ilícita concretada mediante un computador. Asimismo, Temperini (2018) Cuando relacionamos al cibercrimen, estamos citando de una lista de delitos informáticos que ocurren de una forma más profesional, coordinado, la motivación es exclusivamente monetaria, donde los sujetos pasivos de los delitos son componentes fungibles y sin utilidad para el ciberdelincuente, que busca mejorar su rendimiento a través del perfeccionamiento de distintas técnicas delictivas utilizando a la tecnología como eje. En ese mismo orden de ideas, Grenni y Fernández (2018) Manifiestan haciendo una distinción desde la precisión del delito, podríamos evidenciar que el delito informático es una conducta típica, antijurídica y culpable, que se ejecuta utilizando artificios informáticos, que se puede realizar utilizando el conducto del internet, asimismo puede ser vulnerados por cualquier individuo.

El presente trabajo de investigación se realiza con el planteamiento del problema basado en hechos reales que suceden en la sociedad peruana, con respecto a delitos informáticos y la suplantación de identidad, que realizan los

delincuentes, luego de apropiarse de los datos digitales de las personas, para realizar transacciones comerciales, préstamos de dinero, compra y venta de objetos de valor en tiendas por departamentos, transferencias de dinero a otras cuentas, que realiza el delincuente luego de obtener los datos personales de la víctima.

En ese sentido, el problema del trabajo de investigación ¿Cómo se manifiesta la ineficacia de la Ley N°30096, en el delito de suplantación de identidad por medios informáticos?, siendo su objetivo principal advertir las inconsistencias que existe en la ley N°30096, de delitos informáticos con respecto a la suplantación de identidad y los cibercrímenes que llevan a cabo los delincuentes después de obtener toda la información digital de la víctima.

Es de suma importancia, advertir las inconsistencias de la Ley N°30096, de los delitos informáticos con respecto a la suplantación de identidad que efectúan los ciberdelincuentes, específicamente sobre el phishng, vishing y hacker

II. MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Para Aguilar (2019),en su tesis en México “Concluye que nuestras actividades diarias han generado, que se logre exponer nuestra identidad y datos personales via digital, en muchas ocasiones las redes sociales han sido un medio esencial para que los ciberdelincuentes utilicen los datos personales, creen perfiles falsos y vulneren la identidad de sus víctimas, el robo de la identidad hace referencia a lo ilícito que se realiza con la afectación de la persona por ejemplo, cuando se compra utilizando una tarjeta de crédito, introducimos a un POS o el empleado pasa por la ranura de la caja de pago, nuestros dato personales pueden ser vulnerados, ser clonada y utilizada de manera fraudulenta, cuando se realiza un trámite bancario se brinda información personal el que tiene que ser corroborado con un documento oficial, el cual identifica a la persona, para evitar la usurpación y robo de identidad.

Montaperto (2018), en su tesis en Argentina Concluye que los delitos informáticos son crímenes electrónicos el cual llega hacer una dificultad, para el desarrollo de la informática. Por ende, es factible de poseer delitos tan serios como la sustracción de la identidad o falsificación de información, Sin embargo, el extraer información de computadoras o servidores para vulnerar la identidad de una persona cada vez está siendo acechada por ciberdelincuentes, que incurren en este tipo de delitos teniendo la habilidad para direccionar y controlar los diversos programas informáticos. Sin embargo el desconocimiento del marco jurídico regulatorio del art. 18 de la Constitución Nacional como en los tratados con jerarquía constitucional del art. 75 inc. 22 de nuestra carta magna, el agraviado desconoce sobre el proceso que debe seguir al percatarse que la información de su identidad ha sido vulnerado, el sistema de justicia es insípido con la ciberdelincuencia, los delitos informáticos están tomando mayor territorio vulnerando la normativa, el fin es garantizar la protección de los derechos y obligaciones de los ciudadanos, y se deslice con forme a las Leyes Nacionales, Convenios y Pactos Internacionales.

Carriedo (2022) en México indica, Los delitos informáticos o los ciberdelitos se dan por una mala regulación de las nuevas tecnologías de información y comunicación (TIC), los ciberdelitos restringen la información de internet buscando su objetivo y vulnerando la intimidad de una persona utilizando sus datos, las normas mexicanas buscan hacer frente a delitos cibernéticos y salvaguardar la identidad de los ciudadanos. El intento por regular la información personal es muy latente la información que se presenta en las redes sociales (páginas web, Facebook Instagram y Twitter) son vulnerados o modificados por ciberdelincuentes que tiene la habilidad de distorsionar la información y exponiendo tus datos personales generando un daño irreversible.

Chiluisa (2021) en ecuador señala, que, debido al avance tecnológico a gran medida, trajo consigo delitos cibernéticos que transgreden el derecho de intimidad de las personas, de las cuales afecta tanto a persona naturales como jurídicas. Es por ello, que el sistema jurídico ecuatoriano se ve en la obligación de establecer una reforma a la legislación penal en cuanto a la tipificación de delitos, que vayan acorde con la evolución social y tecnológica que acarrea delitos cibernéticos generando que estos no queden impunes y siendo sancionados; establecer una normativa para que sea sancionado el uso fraudulento de las redes sociales, de los sistemas informáticos que dejan en vulnerabilidad a las personas, generando a que estos sistemas sean fácil de ser manipulables y se concrete el delito cibernético.

Santos (2020) en República dominicana indica, que el fin de este análisis, es instaurar nexos probatorios idóneos que sirvan, para sancionar estos delitos electrónicos, ya que muchas demandas no suelen proceder por falta material probatorio, y es que lo primordial de los delitos electrónicos en la República dominicana son el jaqueo de cuentas de redes sociales, correos electrónicos, etc. Los objetivos esenciales que ayudarán con la problemática sobre la sustentación de los medios probatorios idóneos son: conceptualizar las políticas reglamentarias de los delitos electrónicos de la República Dominicana; Conocer el indicador de cibercriminalidad del Distrito Nacional; y valuar los medios probatorios que se presentan para probar los delitos electrónicos. Las investigaciones son dadas en campo y documental la primera, presenta documentos fehacientes y propios como fuente de información la segunda, se basa en la legislación dominicana; pero, estás investigaciones se complementan ya que la investigación de campo al extraer

información es de manera documental, necesita una de la otra, lo que da una complementación de la investigación.

Bechara et. al, (2020) en Colombia señala que la eventualidad de planificar los hechos informáticos como ataques permite, inclusive, que los desarrollos virtuales sean presentados cuando el individuo no se encuentra consciente, esté dormido o imposibilitado para tener una injerencia física o para programar una verificación real sobre las conductas punibles. Entonces se puede decir que las técnicas que utilizan los ciberdelincuentes pueden lograr a traducir la información sin que el autor logre percatarse que su computadora o laptop está en uso, utilizando redes de computadoras que se encuentran infectados.

2.1.2. Antecedentes nacionales

Mori (2019) Indica los desaciertos del desempeño de los operadores de justicia (Policías, Fiscales y Jueces) en él desarrollo y juzgamiento de los delitos informáticos en el resguardo penal de la intimidad, en el Distrito Judicial de Lima., Se concluye que los delitos informáticos se dan a causa de la vulneración de información personal y violación de la intimidad obteniendo como instrumento la conceptualización de antecedentes donde se evidencia la validez del instrumento la cual genero al unir los datos en un tiempo récord, según la peculiaridad de la investigación sobre delitos informáticos.

Alarcón y Barrera (2017) concluye que los delitos informáticos se inician por el uso de la tecnología de información y comunicación, el cual vulnera los derechos constitucionales de los ciudadanos, como el correo electrónico, transacciones financieras y la utilización de las redes sociales que a lo largo del tiempo se está volviendo un instrumento indispensable, para el ser humano, de acuerdo a la naturaleza de las infracciones informáticas se presentan normas para sancionar y evitar la trasgresión de los derechos constitucionales del individuo vulnerado . Así mismo el desarrollo del internet con respecto a las competencias nacionales por destreza se evidencian en un nivel mesurado con el 48%, las competencias informacionales por acceso en un nivel bajo del 40% y las competencias informacionales por aspectos sociales en un nivel templado del 63%. Esto significa que el uso informal de la red social se encuentra en un 63 % el cual la ciberdelincuencia se está aprovechando.

Monja (2022), señala que los delitos informáticos se enfocan en la suplantación de identidad utilizando los sistemas digitales, como resguardo para no ser identificados vulnerando la información de la persona, convirtiéndose en una víctima el cual no puede identificar al delincuente que se encuentran vulnerando, su información. Por ello los bancos adquieren equipos biométricos, que mediante este dispositivo realizan la identificación de la persona, pero no siempre es efectivo, En nuestro país el DNI ha tenido cambios para resguardar la identidad de las personas, hasta llegar a incorporar un chip, en el DNI cambiando su forma tradicional, por una tarjeta de material plástico desarrollando modernas medidas de protección lo cual se innova del antiguo DNI conocido este como un DNI electrónico. Mediante estos cambios y modificaciones su objetivo es proteger la integridad del individuo para finiquitar el tema de suplantación de identidad, las técnicas de identificación en los países que optan por radicar con el tema de suplantación, es la interactuación y el contacto de las personas Generando la identificación de las mismas.

En la actualidad la pandemia ha generado que las entidades Bancarias opten por tener una verificación de protección más detalladas de sus clientes, esto es requerido por las entidades bancarias para comprobar datos y generar el resguardo de los clientes.

Infante (2019), en su tesis**,** con el desarrollo de la tecnología la informática se ha ido implementando, y configurando eventualidades reales de aplicación y de posibilidades de juegos lícitos e ilícitos, donde se hace evidente el derecho penal para restaurar los diversos resultados de una posicion nueva y de tantas potencialidades en el medio social; siendo los casos más latentes el hurto de la identidad virtual que golpea a nuestra sociedad, con lo cual se puede evidenciar, que no presenta un correcto respaldo de los sistemas informáticos por las constantes afectaciones de los mismos; los datos de una individuo que navega en la red, son vulnerados por terceros individuos con fines ilícitos, generando una escena amplia de delitos informáticos, o actos preparatorios de crímenes por medio de las vías electrónicas, es decir ilícitos digitales. En la actualidad por medio de la

Ley 30096, en cuyo artículo 1, se determina que es objeto de Ley preveer y sancionar las conductas ilícitas que atentan a los sistemas y datos informáticos u otros bienes jurídicos significativos de materia penal, cometidos mediante el uso de la tecnología de información o de comunicación, con el fin de asegurar la lucha real contra la ciberdelincuencia.

Huamán (2020) en su tesis, manifiesta que el ingreso al Convenio de Budapest, ha influido de manera real en el desarrollo de los delitos informáticos, al concentrarse en la adecuación de nuestra normatividad prevista en el mencionado Convenio, establece normas para salvaguardar las evidencias digitales. En el Perú, fueron dos programas como el spyware y ramsoware que afectaron a los usuarios, estos fueron mayormente utilizados para cometer el ciberdelito. La importancia de firmar el Convenio de Budapest es que cuenta con un informe real de delitos informáticos; por ello, requiere de recursos económicos para salvaguardar la información tecnológica de los usuarios frente a estos ciberdelincuentes. uno de los aspectos fundamentales fue la suscripción al convenio de Budapest que permitido el inicio de la ley 30096 y las modificaciones realizadas con la Ley 30171, por ello es necesario que esta se mantenga vigente con la legislación de los países de Sudamérica que se unieron para que el convenio se mantenga uniforme, la ciberdelincuencia es un delito que daña la identidad de la persona y vulnera sus derechos.

Huayre (2021) en su tesis, Los delincuentes tienen la libertad de aprovechar cualquier dispositivo con acceso a la tecnología para cometer estos actos delictivos cibernéticos; sin embargo, el presente trabajo de investigación tiene como objetivo cuestionar hasta qué punto la legislación presenta las iniciativas, políticas criminales y procedimientos que ayuden a combatir estos delitos informáticos .Por ello, se realiza un análisis de la problemática para plantearlo en materia legal, para que existan mejoras o modificaciones para resolver este cibercrimen, donde también va de la mano realizar el trabajo de campo. La globalización en materia tecnológica ha sido de gran avance, más aún cuando a causa de la pandemia, la tecnología fue más usada por compras, pagos y atención al usuario por servicios básicos, etc.; todo era realizado por plataformas digitales, cualquier información o dato estaba al acceso de los ciberdelincuentes, lo que incrementó que existiera

mayor inseguridad referente a la información patrimonial de los usuarios. Es por ello, que se busca que exista un resguardo en el ciberespacio, que los usuarios tengan la seguridad de usar estas plataformas digitales sin que su derecho a la intimidad, información, etc. se vea afectado por el cibercrimen.

.

2.1.3. Marco conceptual

Martins (2022) en noviembre de 2001, el Consejo de Europa presento el texto del Convenio sobre la Ciberdelincuencia. Por ello se evidencian, como uno de los pioneros en tratados internacionales vinculados en materia penal, sobre los delitos informáticos.

Convenio de Budapest (2001) Articulo 08. Fraude informático, tipifica delito en el derecho interno de cada país, los actos deliberados e ilegítimos que generen perjuicio patrimonial a un individuo, realizando el, borrado o supresión de información; mediante inferencia en el desarrollo del sistema informático, con la intención delictiva, con el fin de obtener un beneficio económico

Delitos informáticos en el Perú la Ley 30096, articulo 09, suplantación de identidad, se evidencia cuando el individuo utiliza tecnologías de la información o de la comunicación y suplanta la identidad de un individuo , siempre que de dicha conducta resulte un perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Los delitos informáticos son cada vez más, frecuente en el Perú, en especial la suplantación de identidad, donde el delincuente necesita de una computadora, para realizar el crimen por tal razón es necesario tomar precaución cuando se nos va la señal de nuestro teléfono móvil o nos llega correos engañosos y nos piden información personal.

Laredo et. al 2021 señala que las TIC forman parte del desarrollo que se presenta con el tiempo en nuestras actividades y debemos relacionarnos con ellas, ya que evidencian nuestra capacidad física, mental y la posibilidad del desarrollo social. Es necesario en educación y ámbito laboral, dado como positivo en la innovación y en el proceso de aprendizajes, de trabajos a través de la informática que ayudan a desenvolver todo este proceso.

Cavada (2020) señala que el término “cibercrimen” presenta una carencia universalmente homogénea y verificada por los investigadores en el área, evidenciando un acuerdo entre los mismos en que sería un desarrollo ilegal realizada por el uso indebido de un computador.

Saín (2018) menciona que el resguardo informático es verificado como cualquier acción que impide el desarrollo de operaciones no autorizadas sobre un sistema informático o red.

Por ello, se entiende como medidas preventivas, de corrección destinadas a resguardar los recursos informáticos de una institución sea pública o privada.

La suplantación de identidad se suscita cuando un delincuente logra obtener tus datos personales digitales, generalmente del chip del celular, para luego solicitar un cambio del mismo y luego realizar transacciones comerciales.

Según Martínez (2018) los fraude con tarjetas de débito o crédito, son adulteradas, hurtadas, robadas, u obtenidas ilegítimamente.

Phishing: Es una técnica de fraude informático orientada a vulnerar la identidad al sujeto pasivo. El delito pretende obtener información para engañar a una persona para que revele la información personal al atacante como números de tarjetas de crédito y contraseñas, el Phishing en una de las formas más asiduas y conocidas por el ciberdelincuente. Ramos pg.24

Ciberdelitos: Con la expansión mundial de Internet desde algunos sectores se ha confirmado que ésta facilita la comisión de delitos, aunque su consolidación no haya implicado la aparición de nuevas conductas antisociales o ilícitas. Las clásicas fi guras delictivas, ya presentes antes de su irrupción en nuestra realidad diaria, simplemente se han encontrado con un nuevo canal o medio que facilita enormemente su comisión, aunque también su persecución y enjuiciamiento. Hernández pg.236.

Seguridad informática: se considera una de las interpretaciones donde se hace hincapié en la seguridad informática como bien jurídico colectivo a tutelar, el fin es el ataque con conductas informática. Hernández pg.237

Romero, Figueroa, Vera, Alava, Parrales, Alava, Murillo, Castillo (2018) concluye que los virus informático son uno de los principales conceptos cuando se habla de seguridad informática, manifestando que las computadoras solo captan

códigos binarios como ceros y unos, en el mundo de la tecnología y de la informática existe muchos conceptos como el de los programas, videos juegos, o desarrollos operativos y cualquier clase software.

Artículo 02, de constitución política del Perú evidencia que toda persona tiene derecho, a la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar. El concebido es sujeto de derecho en todo cuento lo favorece.

Identidad electrónica. Es información virtual de una persona, que puede ser contraseña de correos electrónicos, contraseña de redes sociales, clave de acceso a tarjetas crédito, para transacciones bancarias.

Bien jurídico protegido, son los datos personales virtuales, como contraseñas de los correos electrónico o Facebook, clave de acceso al celular, pin o clave de acceso a tarjetas crédito, para transacciones bancarias y comerciales.

Identidad electrónica. Es la información virtual de una persona, que puede ser contraseña a correos electrónicos, contraseña a redes sociales, clave de acceso a tarjetas de crédito, para transacciones bancarias.

Martínez (2018) menciona que el robo, la usurpación o suplantación de identidad es un tema muy relevante combinado con el anonimato toma mayor relevancia el poder obtener información del individuo este delito comprende desde el fraude hasta las actividades terroristas.

Sánchez (2018) señala que el hacking como modalidad delictiva accede a nuevas fronteras de acción, el hackeo, para poder ingresar y controlar los aparatos digitales de a bordo permite que vehículos con seguridad por chip de encendido en la llave o los que tienen encendido por botón se encuentren vulnerados con esta modalidad que se encuentra en desarrollo en mercados negros presenciales y los virtuales en la Deep Web (o la Web profunda).

Ingeniería social. son estrategias digitales que utilizan los ciberdelincuentes, para que mediante engaños obtener datos personales, claves y contraseñas para realizar transacciones comerciales.

Hacker: Lo desarrollan personas con alto conocimientos de informática, que tienen como fin vulnerar las redes sociales como Facebook, correos electrónicos y WhatsApp de su víctima, también ingresan a los sistemas de instituciones públicas y privadas con fines ilícitos.

Vishing: Es un tipo de estafa, que se realiza mediante llamadas telefónicas, con el interés de obtener datos personales y cometer delitos: Robo de datos informáticos y Apropiación de identidad

Clonación de tarjetas: Los estafadores generan la imitación de la banda magnética de una tarjeta y clonan en una tarjeta en blanco, para cometer ilícitos.

Spam: Son llamadas no autorizadas que ingresan a tu celular, con fines comerciales o fines ilícitos, son llamas que caen en el acoso.

SIM SWAPPING: Es un fraude que permite acceder a los criminales robar tu identidad mediante el secuestro del número de teléfono al obtener una imitación de tu tarjeta SIM, el delincuente necesita conocer el número celular, fecha de nacimiento y dirección de tu domicilio, para luego solicitar la copia de SIM a la empresa telefónica de la víctima.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

La investigación desarrollada es de **enfoque cualitativo**, se basa en la realidad subjetiva sin dejar de ser científica, según Barrantes (2014) también es denominado naturalista-humanista o interpretativo, y cuyo interés" se centra en estudio de los significados de las acciones humanas y de la vida social". Asimismo, la investigación es de tipo básico, con el fin de obtener un conjunto de información sobre las formas que se origina los delitos digitales al mismo tiempo, para prevenir a los ciudadanos y poner en conocimientos a las autoridades sobre delitos informáticos y la suplantación de identidad, según Sampieri (2004) la investigación se define como "un conjunto de procesos sistemáticos y empíricos que se aplica al estudio de un fenómeno".

Por ello, nuestra investigación tuvo como diseño específico el análisis documental, Al mismo tiempo dicha investigación tiene como objetivo "Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos".

Por otro lado, Sampieri (2004) considera que **los estudios exploratorios** se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes.

Asimismo, como técnicas de investigación, se aplicó la entrevista a profundidad el cual busca recabar información de cada entrevistado, asimismo, se realizó la revisión documental para contrarrestar o consolidar el tema de investigación.

Finalmente, de acuerdo con Chávez y Palomino (2019), "para conocer la investigación cualitativa es necesario explorar las percepciones, opiniones y preferencias de las personas. Por lo tanto, se deben aplicar las siguientes herramientas: Focus group, entrevistas a profundidad y entrevistas a expertos" (p. 64).

3.2. Categorías, Subcategorías y matriz de categorización

Tabla 1

Título: Análisis jurídico de la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.					
Problema	**Objetivos**	**Hipótesis**	**variable**	**Categorías generales**	**Categorías E.**
¿Cómo se manifiesta la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos? **¿De qué manera incide la ineficacia de la Ley N°30096 en el delito del phishing por medios informáticos?** **¿De qué manera incide la ineficacia de la Ley N°30096 en el delito del hacker por medios informáticos?** **¿De qué manera incide la ineficacia de la Ley N°30096 en el delito de clonación tarjeta de crédito por medios informáticos?**	Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos. Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito del phishing por medios informáticos. Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de hacker por medios informáticos. Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de clonación tarjeta de crédito por medios informáticos.	La ineficacia de la Ley N°30096, incide de forma negativa en el delito de suplantación de identidad por medios informáticos. La ineficacia de la Ley N°30096, incide de forma negativa en el delito de phishing por medios informáticos. La ineficacia de la Ley N°30096, incide de forma negativa en el delito de hacker por medios informáticos. La ineficacia de la Ley N°30096, incide de forma negativa en el delito de clonación tarjeta de crédito por medios informáticos.	La ineficacia de la Ley N°30096.	Tipificación de delitos informativos: El que deliberada e ilegítimamente procura para si o para otro un provecho ilícito en perjuicio de terceros mediante el diseño, introducción, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días _ multa. La ley 30096.	• **Phishing** • **Vishing** • **Robo de datos informáticos** • **Hacker**
			Delitos Suplantación de identidad.	Suplantación de identidad: El que mediante la tecnología de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. Ley 30096.	• **Apropiación de identidad** • **Ingeniería social** • **Clonación de tarjeta de crédito** • **Spam**

3.3. Escenario de estudio

Según CITEC (2018) manifiesta que este mecanismo se utilizara durante casi toda la etapa de construcción del sistema de análisis hasta la implementación de la metodología, se describe las perspectivas posibles del desarrollo de una manera abstracta.

El escenario de estudio realiza un análisis de implementación y uso de la perspectiva en la presente investigación, se tiene como población a los abogados de profesión.

El escenario de estudio de esta investigación es Lima – Perú.

3.4. Participantes

Los participantes 10 abogados con grado de maestría especializado en delitos informáticos. También 6 expertos, para la validación de instrumentos.

Tabla 1

Entrevistados

	Entrevistado	*Profesión*	*Fecha de Entrevista*	*Duración*	*Modo de grabación*	*Peso*	*Codificación*
1	Ivon Carolina Cunyas Quispe	Abogado	15/10/2022	30 minutos	Audio	15.MB	E1
2	Julio Sánchez Gutiérrez	Abogado	20/10/2022	30 minutos	Audio	15.MB	E2
3	María teresa de la cruz	Abogada	21/10/2022	35 minutos	Audio	15.2MB	E3
4	Frank Izaguirre Chumpitaz	Abogado	23/10/2022	32 minutos	Audio	15.MB	E4
5	José Luis Nolasco Zavala	Abogado	23/10/2022	31 minutos	Audio	15MB	E5
6	Melissa Nélida Roca Chuco	Abogada	07/11/2022	31 minutos	Audio	15 MB	E6
7	Deise Díaz Aliaga	Abogada	08/11/2022	36 minutos	Audio	15.5MB	E7
8	Pepe Benites Sapallanay	Abogada	08/12/2022	30 minutos	Audio	15 MB	E8
9	Pilar Yarlequé Prieto	Abogada	22/12/2022	30 minutos	Audio	15MB	E9
10	Juan Antonio oliva Ávila	Abogada	28/12/2022	25 minutos	Audio	12MB	E10

Tabla 3

Criterio de inclusión y exclusión

Criterios	Tipo	Inclusión	Exclusión
1er criterio	**Experiencia laboral**	5 años de abogado independiente	Que no presente 5 años de abogado independiente
2do criterio	**Título profesional**	Que presente el título de Abogado	Que no presente título de abogado
3er criterio	**Experiencia laboral**	Tiempo de experiencia no menor de 5 años	Que no tengan experiencia.
4to criterio	**Especialización**	Especialización con el grado de Magíster etc.	Que no presente el grado de magister.

Tabla 4

Criterios de selección de la muestra en libros

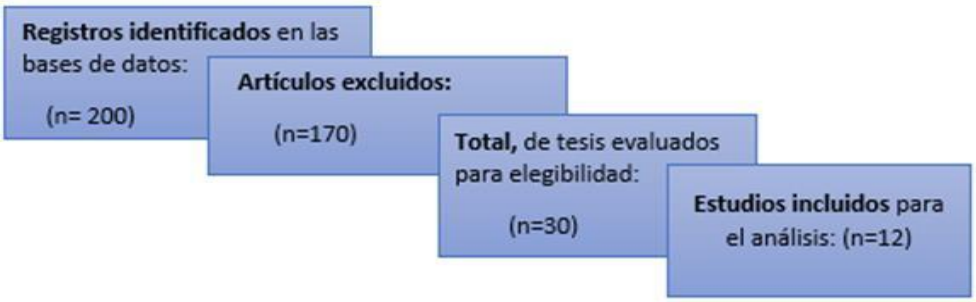
Criterios de Inclusión	**Criterios de Exclusión**
Libro en materia Delitos informáticos.	Libros que no contengan materia Delitos informáticos.
Que se encuentren al alcance en la biblioteca.	Que no se encuentre en la biblioteca.
Ser en idioma español.	Que no contengan el idioma español.
Que contengan información en metodología.	Que no contengan información en metodología.

Finalmente, solo se recolectaron 11 libros que cumplieron con los criterios de inclusión. Por ende, se utilizó en el buscador de Google académico: delitos informáticos- suplantación de identidad, obteniendo un total de 200 tesis. Por ello, para la selección de las tesis se empleó los siguientes criterios de inclusión: a) tesis de la carrera de Derecho, b) que sean del año 2018 en adelante, c) delitos informáticos d) De países Latinoamérica, e) De repositorios f) En idioma español, g) De materia penal y como criterios de exclusión se aplicaron: a) Que no sean de derecho, b) Que no sean del año 2018ª a la posterioridad, c) Aquellos que no contengan el tema delitos informáticos- suplantación de identidad, d) Que no sean de países de Latinoamérica e) Que no se encuentren en repositorios, f) Que no sean en idioma español, g) Todos aquellos que contengan información duplicada y

no aporten nada novedoso. Por ello, solo se incluyeron 12 estudios que cumplieran con los criterios de inclusión (ver Figura 1).

Figura 1

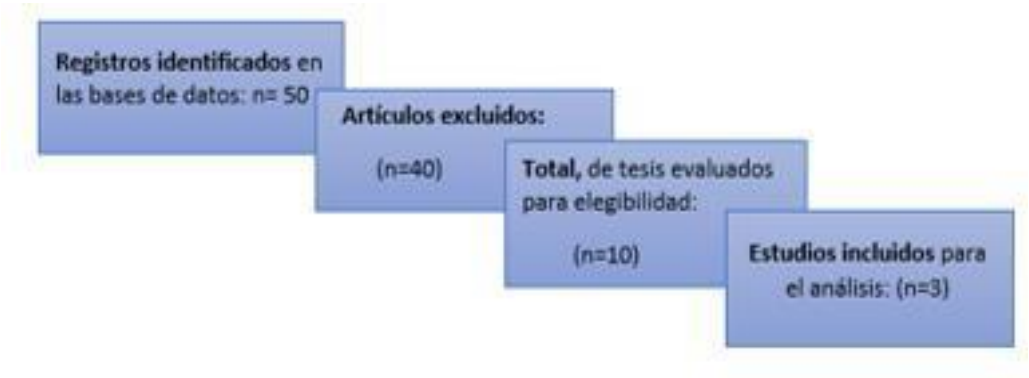
Flujograma de tesis



Asimismo, se anexo tres artículos de la base de datos, el cual cumple con los siguientes criterios de inclusión: a) ser de las ciencias sociales aplicadas, b) ser de la carrera de Derecho y como criterios de exclusión: a) Artículos repetidos, b) Artículos que no sean de Latinoamérica (ver Figura 2).

Figura 2

Flujograma de artículos



3.5. Técnicas e instrumentos de recolección de datos

En la técnica de investigación se contó con la entrevista que es recopilada en base a las respuestas de los magister especializados en delitos cibernéticos; el análisis de documentos y la recopilación de información son datos y guías de análisis de fuente documental.

El Instrumento son recursos que contribuyen a obtener resultados que pueden sustentar el desarrollo de la creación científica Suarez y escudero (2018), el instrumento es una guía de entrevistas para la recopilación de información y procesar los resultados.

Tabla 5

Matriz de ficha técnica instrumental

Aspectos Claves	Instrumento 1	Instrumento 2
Técnica Nombre	Entrevista a profundidad	Revisión Documental
Tipo	Semi – estructurada	Análisis de documental
Instrumento	Guía de entrevista	Guías de revisión
Técnica Objetivo General	Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.	Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito del **phishing** por medios informáticos.
Específico Objetivo	Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito del **phishing** por medios informáticos.	Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito del **phishing** por medios informáticos.
Fuente de procedencia	Propia	Propia
Contenido Multidimensional	12 ítems	2 guías
Tipo de Instrumento	Cualitativo	Cualitativo
Criterio de Validez Expertos	-Alberto remondo ángeles macavilca -Alexander solorzano palomino -Miguel Beltrán montes -Fredesbinda Neira Huaman -Edgar Jesús flores guardia -Edwin flores castillon	-Alberto remondo ángeles macavilca -Alexander solorzano palomino -Miguel Beltrán montes -Fredesbinda Neira Huaman -Edgar Jesús flores guardia -Edwin flores castillon
Muestra de aplicación	• Abogados especialistas • 10 abogados penalistas	• Tesis realizadas con el objeto de estudio de los delitos cibernéticos

Nota: Ficha resumen de las técnicas aplicadas. La tabla ha sido extraída de Desde la idea hasta la sustentación: 7 pasos para una tesis exitosa. Un método efectivo para las ciencias empresariales, (p. 268) por A. Vara Horna, 2012, (3a ed.), Facultad de Ciencias Administrativas y Recursos Humanos, Universidad de San Martín de Porres, Lima.

3.6. Procedimiento

La presente investigación se inició con la presentación del título de investigación y la realidad problemática como también los objetivos, asimismo la presentación del marco teórico con autores nacionales e internacionales que están sustentados mediante el trabajo de la investigación.

Se realizó la metodología de investigación con un cualitativo y de diseño explicativo de tipo básico, Asimismo, se cuenta con la justificación de esta investigación, en relevancia al ámbito de estudio, por otro lado, se realizó la validación de instrumento con expertos, por ello se procedió a realizar una selección de muestra con los magister especializados en delitos cibernéticos, la técnica utilizada es la entrevista a profundidad.

3.7. Rigor científico

La investigación cualitativa, se define por el discernimiento de varios autores, generando distintos parámetros equitativos los de confiabilidad y objetividad, para ello se ha utilizados instrumentos con criterios de credibilidad que han permitido el análisis y el estudio de las categorías.

Asimismo, se enfatizó como instrumentos, la guía de entrevista, se planteó preguntas que responde a nuestros objetivos, la cual fue liderada netamente con expertos en el tema de investigación.

Por ello, se empleó la guía de análisis de revisión documental se realizó un estudio minucioso de la LEY 30096 ley de delitos informáticos referente al delito de suplantación de identidad mediante la tecnología.

V DRE AIKEN	INTERPRETACION
0.00-0.79	DEBIL
0.80-0.89	ACEPTABLE
0.90-1.00	FUERTE

$$\boxed{v =} \frac{S}{n(C-1)}$$

S = Sumatoria de respuestas o acuerdos de los expertos por cada ítem

N = Numero de expertos.

C = Numero de valores en la escala de la V de Aiken

Por otro lado, se llevó a cabo la validación de la guía de entrevistas que se presentara:

Este instrumento contiene cuatro (4) ítem; ítem 8; ítem 10; ítem 11; ítem 12), con una validez de contenido fuerte, debido que el coeficiente se ubica en el intervalo de 0.90 a 1.00, lo que se interpreta que todos los expertos están completamente de acuerdo

Asimismo, el instrumento contiene ocho (7) ítems (ítem 1, ítem 2, ítem 4; ítem 5; ítem 6; ítem 7; ítem 9;) que presentan una validez de contenido aceptable de intervalo de 0.80-0.89 indicando de los expertos están de acuerdo.

A pesar de ello es necesario mencionar que el instrumento contiene un (1) ítem, con una validez de contenido débil, debido a que el coeficiente se ubica en el intervalo de 0.00 a 0.79, lo que indica que los 6 expertos están en desacuerdo, pero no tiene que modificarse ya que solo es una pregunta inductiva y no afecta el fondo de la validez y confiabilidad del instrumento.

Finalmente, el instrumento de investigación tiene coeficiente de validez de contenido 0.89 que es aceptable, debido a que el coeficiente se ubica en el intervalo0.80-0.89, por lo que también se muestra que el coeficiente de validez tiene un contenido de (1.00) es fuerte, debido a que el intervalo es de 0.90 a 1.00, por lo que resulta acto para la aplicación del instrumento.

3.8. Método de análisis de datos

En análisis cualitativo se constituyó mediante una estructura para ello se contó con búsqueda de base de datos poder documentar este proceso, asimismo, la presente investigación implico la recopilación de información, e interpretación de los resultados con el fin de obtener una visión amplia de el objeto de estudio.

Es preciso indicar que la investigación conto con entrevistas de manera individual con especialistas capacitados en el tema de delitos informáticos las cuales nos permitió el mejor desarrollo y mayor comprensión, donde se podrá aplicar las guías de matriz de entrevistados.

3.9. Aspectos éticos

El proceso de investigación cumple con los estándares establecidos por el enfoque cualitativo con una revisión de documentales realizando un análisis de dato cumpliendo con lo requerido por el código de ética de la UNIVERSIDAD CESAR VALLEJO.

Asimismo, se ha seguido los estándares establecidos por la propiedad intelectual, utilizando de forma objetiva la información proporcionada por la casa de estudio y el asesor metodológico, de igual forma de utilizo las normas APA establecida de acuerdo a la normativa, es preciso indicar que se ha utilizado los estándares de derecho de autor por lo cual se respetó las reglas del fondo editorial UCV.

Por otro lado, la problemática que se desarrollo fue accesible de ser estudiada y se contó con los recursos necesarios para el desarrollo eficaz, asimismo, se tiene presente el compromiso de entorno a la información proporcionada.

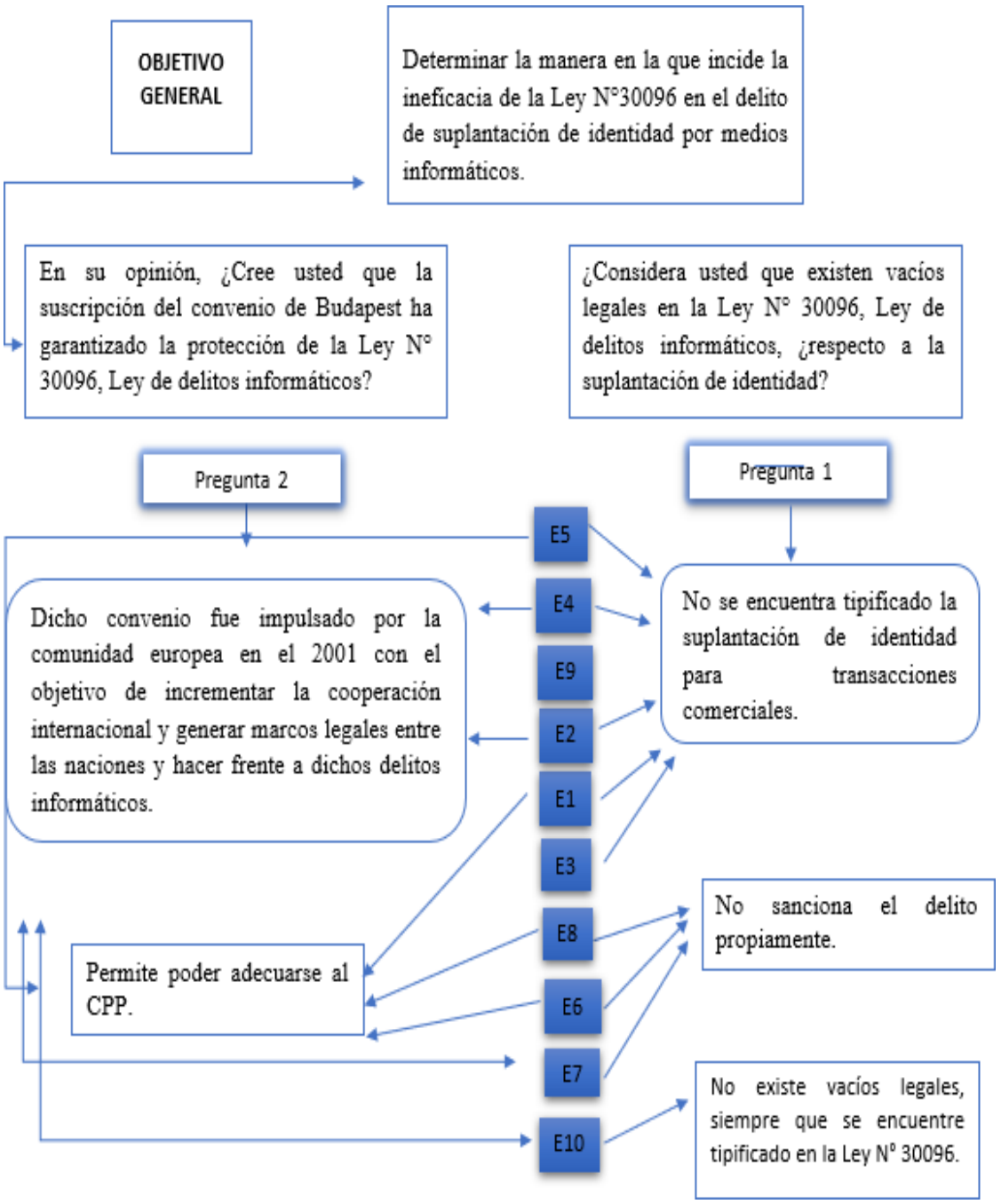
IV. RESULTADOS Y DISCUSIÓN

Los resultados de la investigación se realizaron en base a los objetivos y las respuestas de los entrevistados, resaltando principalmente aquellas que responden a los objetivos, ya que las demás respuestas serán de respaldo (ver Anexo 5).

Con respecto al objetivo general, los entrevistados respondieron la pregunta 1, de la siguiente manera: No se encuentra tipificado la suplantación de identidad para transacciones comerciales, asimismo consideran que no sanciona el delito propiamente, por otro lado, el E10, considera que No existe vacíos legales siempre que se encuentre tipificado en la Ley N° 30096. En cuanto a la pegunta 2, los entrevistados coinciden que Dicho convenio fue impulsado por la comunidad europea en el 2001 con el objetivo de incrementar la cooperación internacional y generar marcos legales entre las naciones y hacer frente a dichos delitos informáticos con el fin de adecuar a la CPP.

Figura 3

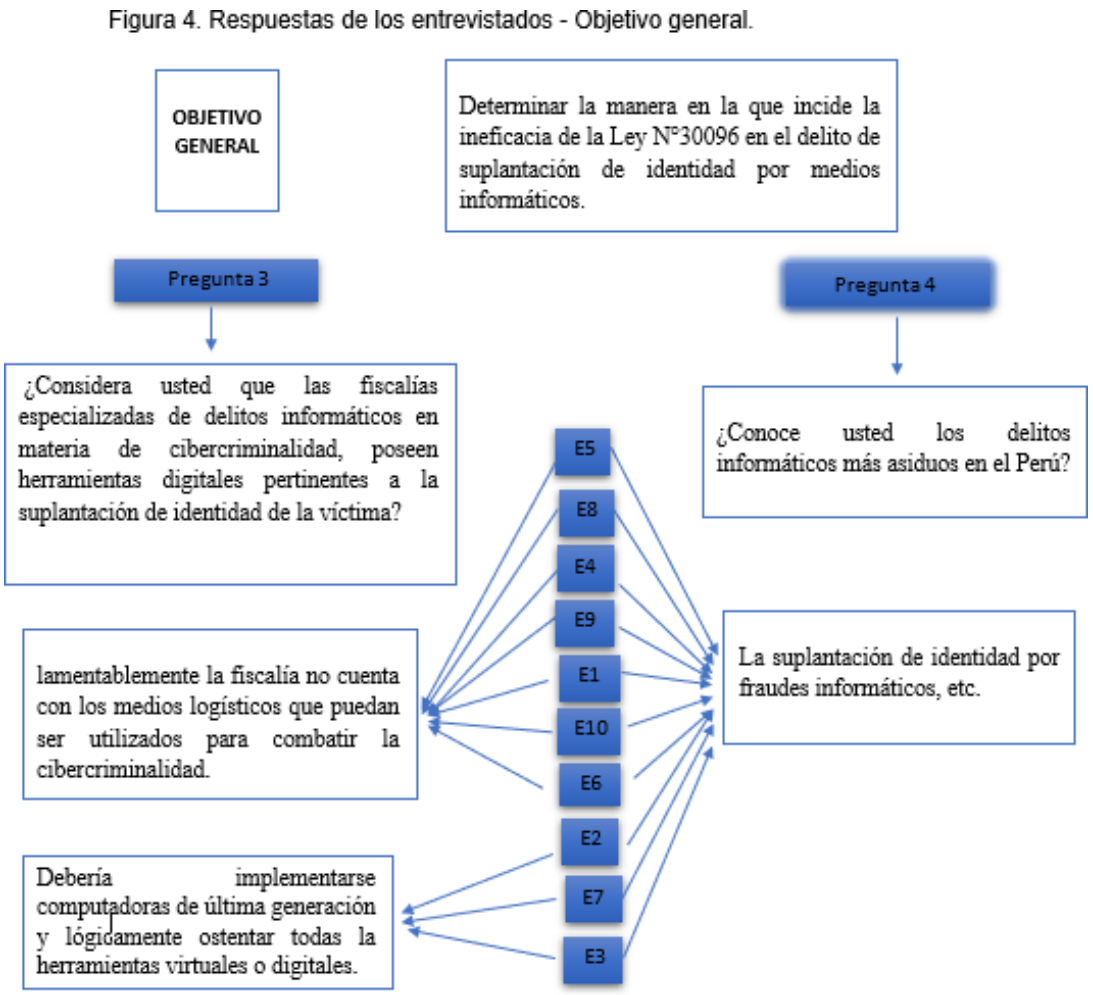
Respuesta de los entrevistados – Objetivo general



Con respecto al objetivo general los entrevistados respondieron la pregunta 3 de la siguiente manera: para un grupo de participantes consideran que lamentablemente la fiscalía no cuenta con los medios logísticos que puedan ser utilizados para combatir la cibercriminalidad (E10, E9, E8, E5, E4, E3y E1) otro grupo considera que debería implementarse computadoras de última generación y lógicamente ostentar todas la herramientas virtuales o digitales. (E7; E6, E3 y E2) En cuanto a la pegunta 4, todos los entrevistados coinciden que los delitos informáticos más asiduos son: La suplantación de identidad por fraudes informáticos, etc.

Figura 4

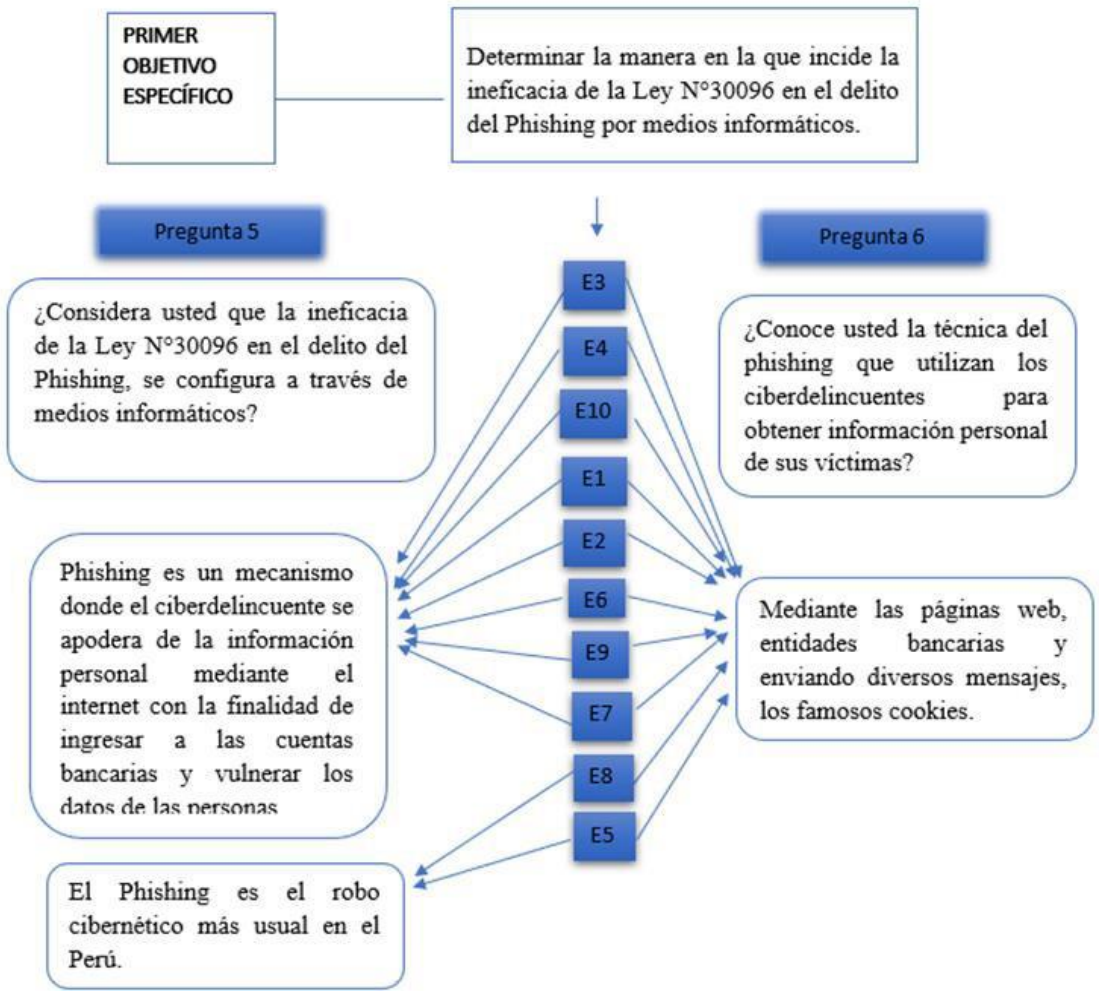
Respuestas de los entrevistados – Objetivo general.



Respecto al primer objetivo específico, los entrevistados respondieron la pregunta 5, de la siguiente manera: el Phishing es un mecanismo donde el ciberdelincuente se apodera de la información personal mediante el internet con la finalidad de ingresar a las cuentas bancarias y vulnerar los datos de las personas (E7,E6,E4,E3,E2 y E1) , otro grupo considera que el Phishing es el robo cibernético más usual en el Perú (E8 y E5) En cuanto a la pegunta 6, Todos los entrevistados coinciden que los ciberdelincuentes utilizan las técnicas mediante las páginas web, entidades bancarias y enviando diversos mensajes los famosos cookies.

Figura 5

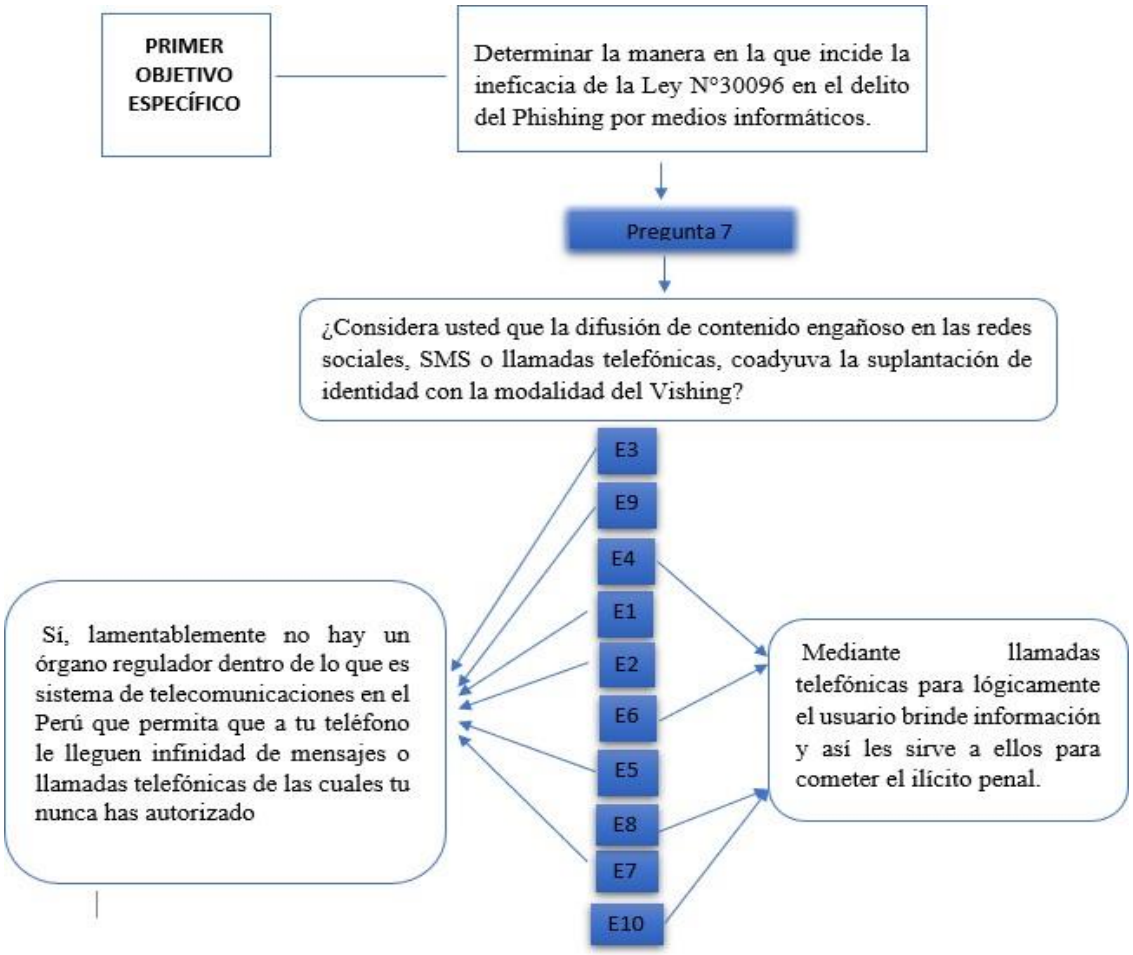
Respuesta de los entrevistados – Objetivo específico 1.



Respecto al primer objetivo específico, los entrevistados respondieron la pregunta 7,de la siguiente manera lamentablemente no hay un órgano regulador dentro de lo que es sistema de telecomunicaciones en el Perú que permita que a tu teléfono le lleguen infinidad de mensajes o llamadas telefónicas de las cuales tu nunca has autorizado (E7,E5,E3,E2 y E1) otro grupo de entrevistados considera que utilizan la modalidad del Vishing Mediante llamadas telefónicas para lógicamente el usuario brinde información y así les sirve a ellos para cometer el ilícito penal (E9,E10,E8,E7,E6 y E4)

Figura 6

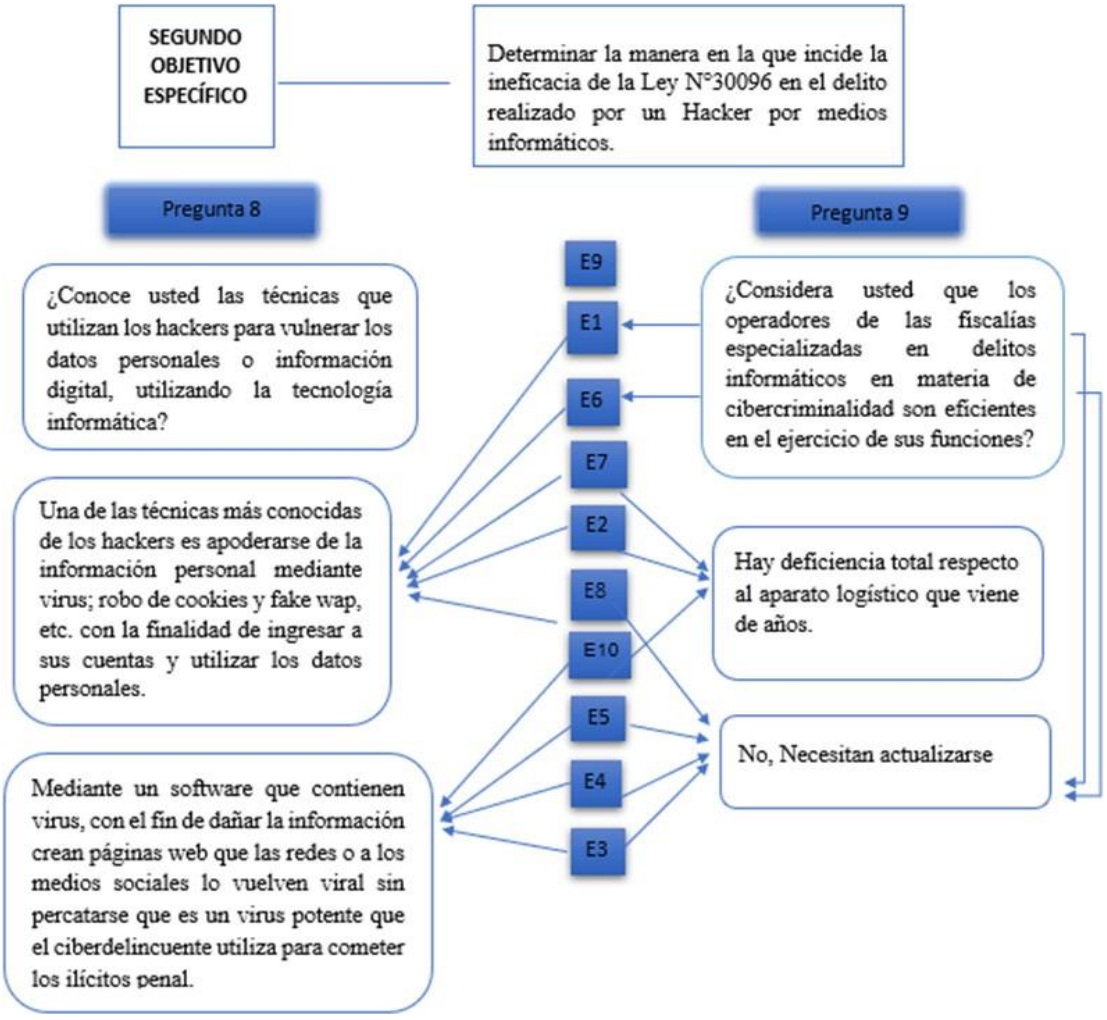
Respuestas de los entrevistados – Objetivo específico 1.



Con respecto al objetivo específico 2, los entrevistados respondieron la pregunta 8, de la siguiente manera: Una de las técnicas mas conocidas de los hacker es apoderarse de la información personal mediante virus ; robo de cookies y fake wap,etc con la intención de ingresar a sus cuentas y utilizar los datos personales E9,E6,E7,E2 y E1) otro grupo de entrevistados considera que Mediante un software que contienen virus, con el fin de dañar la información crean páginas web que las redes o a los medios sociales lo vuelven viral sin percatarse que es un virus potente que el ciberdelincuente utiliza para cometer el ilícito penal (E10,E8,E5,E4 y E3) En cuanto a la pegunta 9,los entrevistados consideran que hay deficiencia total respecto al aparato logístico que viene de años.(E7,E6 y E8) otro grupo de entrevistados consideran que Necesitan actualizarse (E5,E4 y E2).

Figura 7

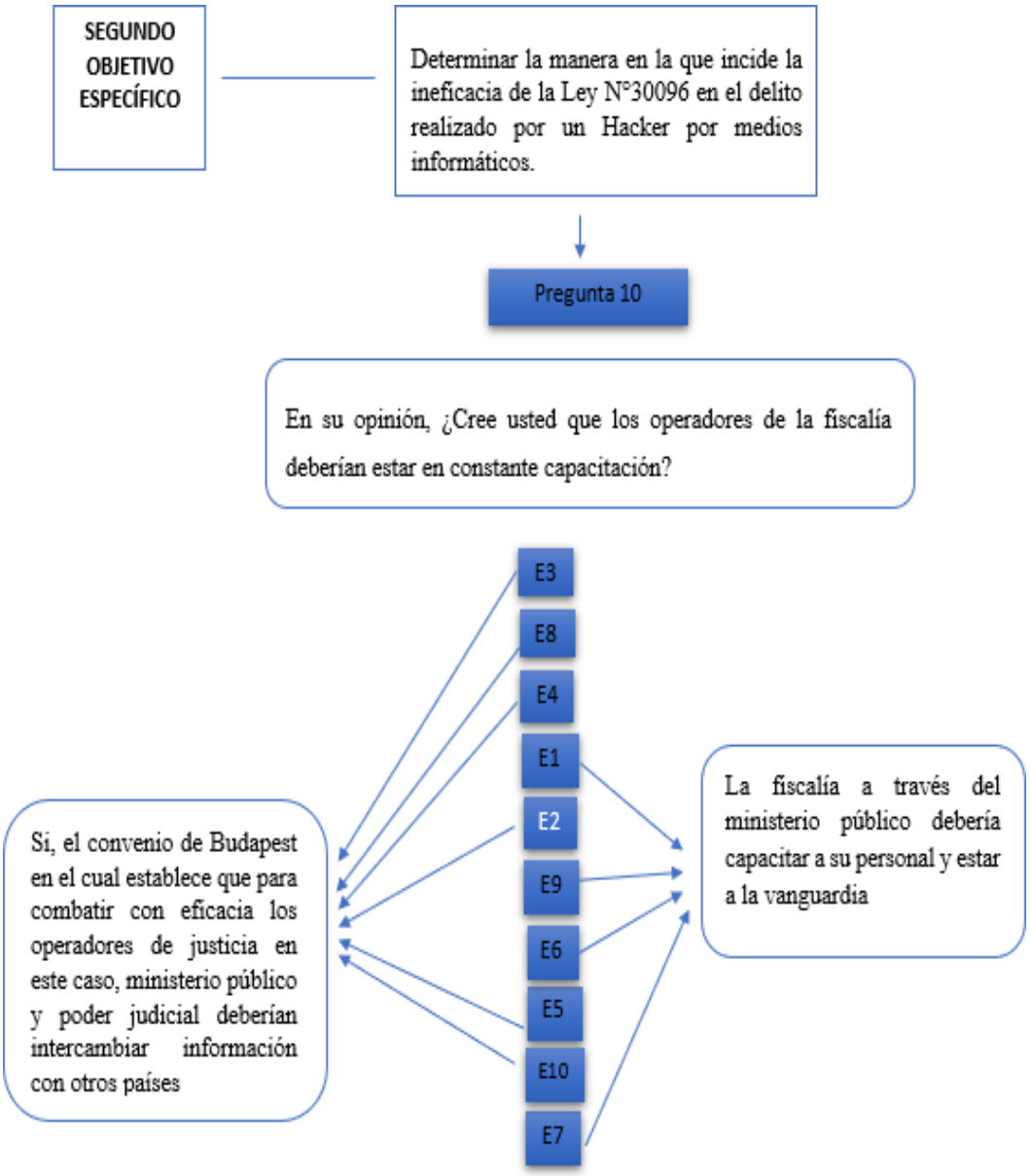
Respuesta de los entrevistados – Objetivo específico 2.



Con respecto al objetivo específico 2, los entrevistados respondieron la pregunta 10, de la siguiente manera: el convenio Budapest establece que para combatir con eficacia los operadores de justicia en este caso ministerio público y poder judicial intercambien información de con otros países (E10,E8.E5,E4 y E3) otro grupo de entrevistados considera que la fiscalía a través del ministerio público debería capacitar a su personal y estar a la vanguardia (E9,E7,E6 y E1)

Figura 8

Respuesta de los entrevistados – Objetivo específico 2.



Respecto al objetivo específico 3, los entrevistados respondieron la pregunta 11, de la siguiente manera: No, pero me envían correos maliciosos. (E1,E2,E3.E4.E5,E6,E7,E8,E9 y E10) En cuanto a la pegunta 12,los entrevistados consideran que prefieren realizar una compra presencial es decir directamente puesto que presumen que si lo hicieran de manera online lógicamente no se sienten protegido(E1,E2,E3.E4.E5,E6,E7,E8,E9 y E10)

Figura 9

Respuesta de los entrevistados – Objetivos específico 3.

Por otro lado, se prosiguió a evidenciar los resultados de la guía de revisión documental, la cual presenta libros, articulo y tesis que se utilizó, la cual fue necesaria para argumentar y dar respuesta a los objetivos de investigación (ver Anexo 5).

Tabla 6

Matriz codificada de resultados de libros.

CODIFICACIÓN	CONCLUSIONES
L1	C1. La tecnología informática genera su influencia en la mayoría de las áreas estas han surgido una lista de comportamientos en algunos casos es difícil tipificación en las normas penales, sin recurrir al principio de legalidad.
L2	C2. Es necesario realizar un proceso de identificación y evaluación de diferentes riesgos informáticos.
L3	C3. Los trabajadores desconocen las herramientas y presentan dificultades en el flujo de información, es necesario mejorar la eficiencia poniendo en práctica todas las herramientas digitales.
L4	C4. La problemática jurídica de los sistemas informáticos tiene que considerar la tecnología de la información en su totalidad (inteligencia artificial, redes, microprocesadores, etc.) para así obtener medios probatorios que permitan la detección de los ilícitos que se hayan cometido utilizando ordenadores.
I5	C5. Los hackers especializados en sistemas avanzados su objetivo es vulnerar sistemas remotos con la creación de virus o crack de software, considerados el grupo mas experto y menos ofensivo.
L6	C6. Un usuario novato tiene problemas al enfrentarse a un virus este puede ser introducido a la memoria interna de un ordenador que al activarse puede destruir totalmente o parcialmente tu información.
I7	C7. La normativa referida a la ciberdelincuencia tal con la ley N° 30096 Ley de delitos informáticos o la ley N° 30999 Ley de ciberdefensa, asimismo nos encontramos dentro del convenio Budapest, para generar un mejoramiento e incorporaciones de diverso de componentes vinculados al análisis de la ciberdelincuencia.
I8	C8. Las pruebas de materia informática pueden plantearse como un recurso digital, donde la destreza del investigador y el desarrollo de herramientas dará un resultado exitoso.
I9	C9. El avance de las redes informanticas genera que los funcionarios se encuentren capacitados para unificar criterios de investigación.
I10	C10. La tecnología y la información desmesurada genera el promover las condiciones de seguridad
I11	C11. Es necesario reforzar la seguridad de las PC, para proteger de los hacker y piratas informáticos, que podrían paralizar el sistema de tu ordenador.
I12	C.12 El delito informático es la acción u omisión realizada por un individuo que con la intención de causar perjuicio a una persona o aun conjunto de personas, generando su beneficio propio.

Tabla 7

Matriz codificada de resultados de artículos.

CODIFICACIÓN	CONCLUSIONES
A1	C1. La criminalidad informática consiste en el comportamiento ilícito C2. Se atentando con la seguridad de los datos procesados. C3. Se realiza la alteración de los datos informáticos.
A2	C1. Los delitos informáticos se conjugan en el sistema dogmático C2. El mundo cibernético establece un sistema sin control. C3. EL ID del usuario no genera seguridad en la criminalidad informática
A3	C1. La tecnología informática configura una realidad de un mundo globalizado. C2. El desarrollo cibernético establece exigencias globalizadas. C3. La protección de la tecnología persigue conductas antijuridicas

Tabla 8

Matriz codificada de resultados de tesis.

CODIFICACIÓN	**CONCLUSIONES**
T1	C1. Las redes sociales con el tiempo se hacen necesarios para la sociedad el cual son vulnerados por la ciberdelincuencia captando la información personal y exponiendo la identidad.
T2	C1. El agraviado desconoce del marco jurídico y de los avances de la ciberdelincuencia.
T3	C1. La información tecnológica se configuro como necesaria e indispensable para el ser humano.
T4	C1. El uso indebido de la tecnología de información genera un instrumento de vulneración de datos personales e identidad de la víctima.
T5	C1. Las TIC son vulnerados por los delitos informáticos, la información personal se regula como endeble y la tente para el ciber delincuente.
T6	C1. La naturaleza jurídica se encuentra afectado por la ciberdelincuencia, se vulnera el derecho a la intimidad de las personas, sancionar el uso fraudulento de las redes sociales.
T7	C1. Los delitos informáticos no logran ser sancionados por falta de medios probatorios.
T8	C1. La suplantación de identidad en el sistema bancario genera que el ciberdelincuente utilice diversos sistemas digitales para no ser identificados vulnerando la información de una persona.
T9	C1. Es necesario realizar un proceso de concientización de protección de datos en las redes sociales, las redes evidencian contenidos denominados “fake” utilizando la identidad de una persona suplantando su identidad.
T10	C1. El principio de legalidad enfocándose entorno a la suplantación de identidad considera una conducta atípica, por la falta de tipo y sanción penal.
T11	C1. El robo cibernético se manifiesta como una conducta indebida, será sancionada toda vez que se encuentre las pruebas que se utilizaron para su beneficio propio con el fin de vulnerar la información de la víctima
T12	C1. La suplantación de identidad es una conducta indebida, será sancionada toda vez que se encuentre las pruebas que se utilizaron para su beneficio con el fin de vulnerar la información de la víctima de manera ilícita.

Figura 10

Tesis y artículos recolectados.

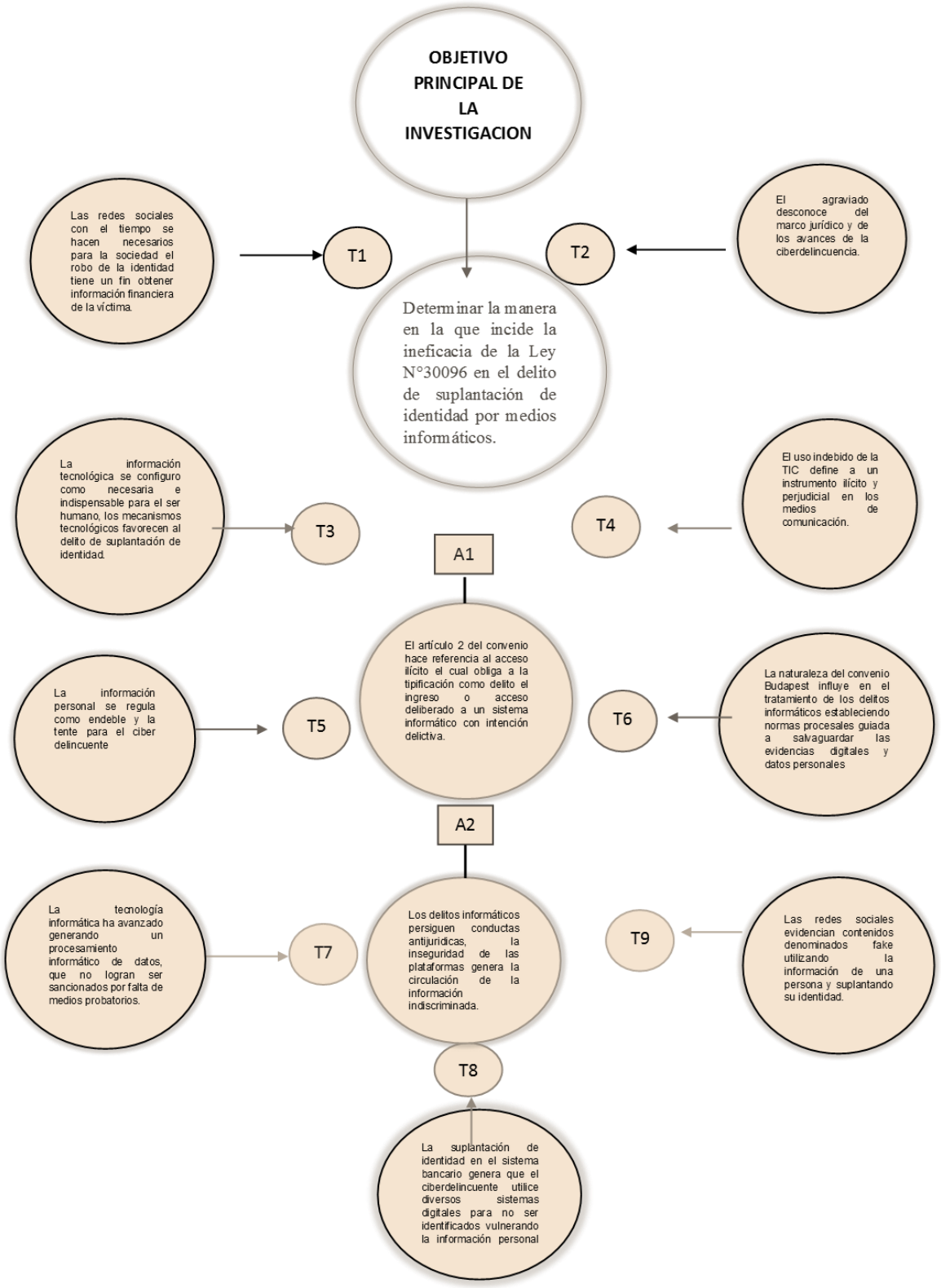


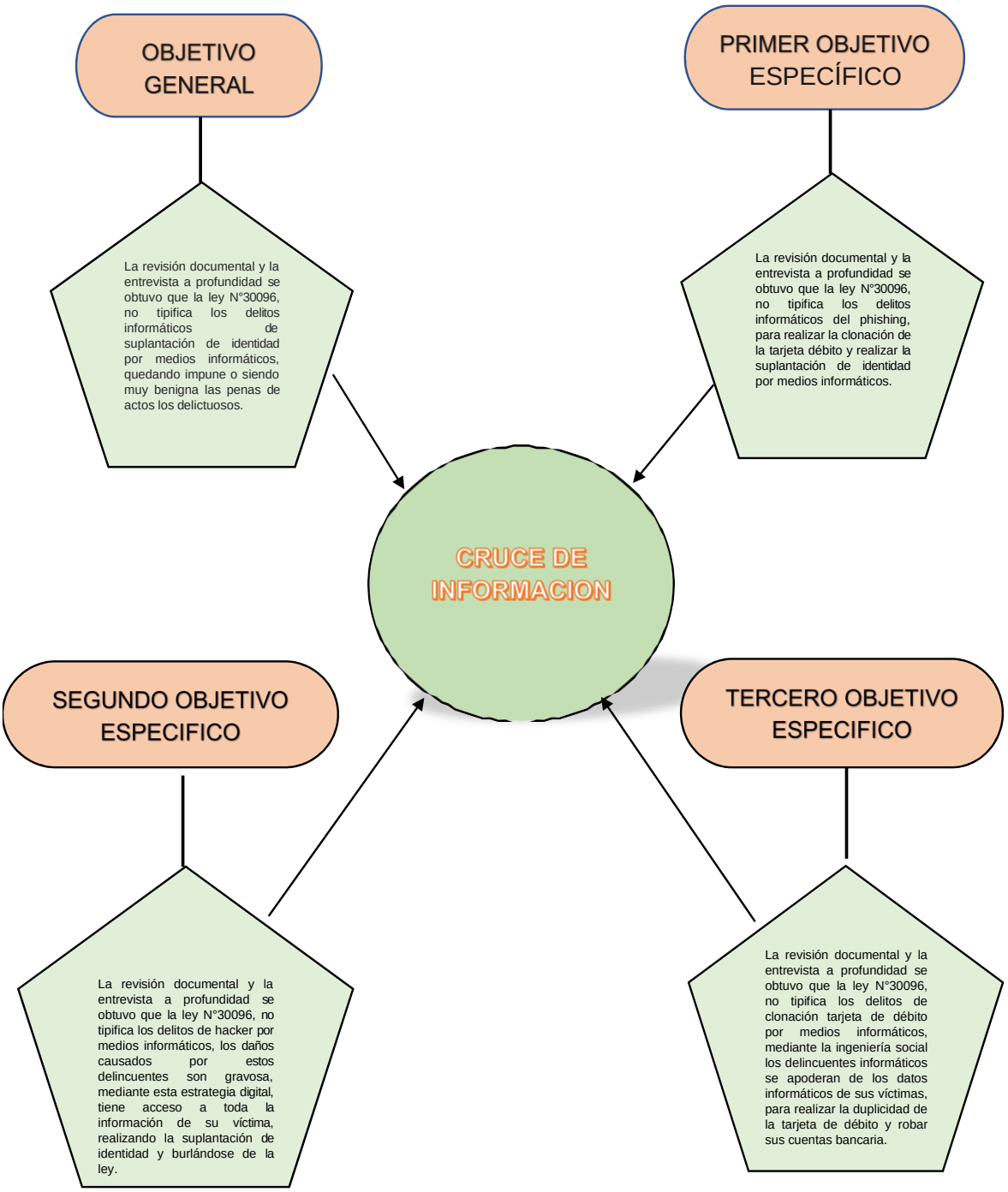
Tabla 9

Matriz de triangulación.

	CATEGORÍAS	**ESPECÍFICAS**		
V. INDEPENDIENTE	GENERAL	**Phishing**	**Vishing**	**Hacker**
Análisis Jurídico de la ineficacia ley 30096	Análisis Jurídico de la ineficacia ley 30096	RD: Indican que son correos maliciosos, se hacen pasar por bancos o instituciones del estado, ofertando premios, para luego sus datos digitales. E: manifiestan que, si conocen el phishing, es una forma de robar los datos personales de una persona, para luego suplantar su identidad. (E1, E2,…..E10)	RD: se puede notar que son llamadas maliciosas, donde solicitan datos digitales, se hacen pasar por instituciones bancarias. E: señalan que el envió de llamadas telefónicas, que nunca se autorizó, buscando estafar a las personas. (E1, E2,…..E10)	RD: son expertos en computación ingresan a los correos, Facebook y cuentas bancarias de las personas con fines ilícitos. E: Manifiestan que Vulneran principalmente las cuentas bancarias, para realizar transferencias de dinero no autorizadas. (E1, E2,E10)
V. INDEPENDIENTE	GENERAL	**Apropiación de identidad**	**Ingeniería social**	**Clonación de tarjeta de debito**
Suplantación de identidad	Suplantación de identidad	RD: Mediante la tecnología de la información suplantan la identidad, a una persona natural o jurídica, resultando dicha conducta perjuicio económico a la persona. E: Indican que los delitos más concurrentes son la suplantación de identidad, se inicia con el robo de datos digitales de las personas. (E1, E2, E10)	RD: Es una estrategia que utiliza los delincuentes, para engañar y obtener los datos digitales de las personales de sus víctimas. E: Señalan que son estrategias que utilizan los delincuentes, para engañar a sus víctimas, y robar sus datos personales. (E1, E2, E10)	RD: después de obtener los datos de sus víctimas, realizan la clonación de la tarjeta débito. E: Manifiestan que no fueron víctima, pero que sus familiares y amigos, duplicaron su tarjeta para robar vaciar sus cuentas bancarias. (E1, E2,…..E10)

Figura 11

Cruce de información.



4.1. Discusión

Obtenido los resultados de los entrevistados se pasará a la etapa de discusión comparando, contrastando y demostrando en base a los objetivos y la verificación con la hipótesis de la investigación.

En relación con el objetivo general: Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.

En relación la hipótesis general: La ineficacia de la Ley N°30096, incide de forma negativa en el delito de suplantación de identidad por medios informáticos.

Los resultandos indican que existe ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos, no se encuentra tipificado las transacciones comerciales, tales como la compra y venta por internet, transferencia de dinero a otras cuentas que realiza los delincuentes, luego de sustraer los datos digitales de sus víctimas (Nolasco; Izaguirre; Cunyas; Diaz; De la Cruz; Roca y Sánchez; 2022) (ver Anexo 4)

Un resultado similar obtuvo Montaperto (2018), Concluye que los delitos informáticos son crímenes electrónicos el cual llega hacer una incertidumbre, para el avance de la informática. Por ende, este puede ocasionar delitos tan graves como el robo de la identidad y falsificación de información, Sin embargo, el extraer información de computadoras o servidores para vulnerar la identidad de una persona cada vez está siendo acechada por ciberdelincuentes. Sin embargo, el desconocimiento del marco jurídico regulatorio del art. 18 de la Constitución Nacional como en los tratados con jerarquía constitucional del art. 75 inc. 22 de nuestra carta magna, el agraviado desconoce sobre la diligencia que debe seguir al percatarse que la información de su identidad ha sido vulnerado, el sistema de justicia es insípido con la ciberdelincuencia, Así mismo en la presente investigación, el delito de suplantación de identidad por medios informáticos, no se encuentra tipificado por tal razón no son sancionados propiamente, las transacciones comerciales, tales como la compra y venta por internet, transferencia de dinero a otras cuentas que realiza los delincuentes, luego de sustraer los datos digitales de sus víctimas (Nolasco; Izaguirre; Cunyas; Diaz; De la Cruz; Roca y Sanchez;2022) (ver Anexo 4)

Resultado similar obtuvo Huamán (2020) manifestando que la suscripción del Convenio de Budapest, repercute de manera relativa en el tratamiento de los delitos informáticos, al enfocarse en la adecuación de la normatividad prevista en el mencionado Convenio, asimismo establece normas para salvaguardar las evidencias digitales.

Por todo ello se concluye, contrasta y corrobora el delito de suplantación de identidad por medios informáticos, no se encuentra tipificado las transacciones comerciales, tales como la compra y venta por internet, transferencia de dinero, por tal razón no son sancionados propiamente los delincuentes cibernéticos, en consecuencia, son liberados puesto que no se encuentra visible en la ley el delito que cometió.

Con respecto al primer objetivo específico: "Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito del phishing por medios informáticos."

Con respecto a la primera hipótesis específico: "La ineficacia de la Ley N°30096, incide de forma negativa en el delito de **phishing** por medios informáticos".

Así mismo en la presente investigación los resultandos indican Phishing un mecanismo donde el ciberdelincuente se apodera de la información personal mediante el internet con la finalidad de ingresar a las cuentas y vulnerar los datos personales (Nolasco Zavala; Izaguirre Chumpitaz; Cunyas Quispe ; Diaz Aliaga; De la Cruz de fuertes; Roca Chuco y Sánchez Gutiérrez (2022) (ver Anexo 4)

Por otro lado, Aldecoa (2021) indica, que el robo de la identidad es uno de los delitos que se ha desarrollado en los últimos años, suele tener un solo objetivo que es el robo de información personal para realizar un perjuicio a un usuario.

Un resultado similar obtuvo Ferro (2020) manifiesta los delitos informáticos se han incrementado debido a la facilidad que tiene el autor del crimen en permanecer en el anonimato, utilizando programas para precisar claves de usuarios, asimismo esconder su identidad y cometer delitos financieros estos son considerados acto de terrorismo. Finalmente, De Sola (2021) señala que la manipulación de los datos de entrada: Este tipo de fraude informático también conocido como sustracción de datos, representa el delito informático más usado ya

que es fácil de cometer y difícil de detectar. Este delito no requiere de conocimientos técnicos de informática puede realizarlo cualquier persona que tenga acceso a una computadora con internet.

Así mismo en la presente investigación los resultados indican El Phishing es el robo cibernético más usual en el ámbito delictivo y en la ciberdelincuencia, (Nolasco Zavala; Izaguirre Chumpitaz; Cunyas Quispe; Diaz Aliaga; De la Cruz de fuertes; Roca Chuco y Sánchez Gutiérrez (2022) (ver Anexo 4)

Resultado similar obtuvo De Sola (2021) indica que la verificación de los datos de entrada, es un tipo de fraude informático también conocido como sustracción de datos, representa el delito informático más empleado, por ello es fácil de cometer y difícil de descubrir. Para este delito no es necesario de una persona que contenga conocimientos de informática puede realizarlo cualquier persona que tenga la habilidad de desenvolverse en el ámbito cibernético.

Por todo esta se concluye contrasta y corrobora el phishing es el robo de información más usual, consiste en enviar correos maliciosos a las personas simulando ser entidades bancarias o instituciones públicas piden validar cierta información, donde solicitan datos personales, para luego utilizarlo en solicitar otro chip a la empresa telefónica y realizar la suplantación de identidad.

Con respecto al segundo objetivo específico: Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de **hacker** por medios informáticos

Con respecto a la segunda hipótesis específico: La ineficacia de la Ley N°30096, incide de forma negativa en el delito de hacker por medios informáticos. Según los entrevistados el hacker es la técnica más conocida del robo de datos digitales, el delincuente vulnera la contraseña de correos electrónicos y redes sociales, principalmente su objetivo es la tarjeta de débito donde se encuentra el dinero de la víctima con el fin de utilizar diferentes modalidades: hurtar el dinero, realizar compras por internet o generar transferencia a otras cuentas bancarias. (Nolasco Zavala; Cunyas Quispe; Diaz Aliaga; De la Cruz de fuertes; Sánchez Gutiérrez y Benites Sapallanay (2022) (ver Anexo 4)

Un resultado similar obtuvo **Martínez (2018)** concluye que el robo, la usurpación o suplantación de identidad es un tema muy destacado, A través de él

anonimato los delincuentes utilizan los datos personales para hacerse pasar por el usuario al que le han vulnerado su identidad. Estos hechos ilícitos se emplean para cometer una serie de delitos que comprenden desde el fraude hasta las actividades terroristas.

Así mismo en la presente investigación los operadores **de justicia,** la fiscalía a través del ministerio público debería de preparar a su personal y estar a la vanguardia en delitos informáticos para valorar las pruebas de dichos delitos que cometen los hackers al vulnerar los correos, redes sociales y cuentas bancarias de la persona, con el objetivo de vaciar los ahorros de sus víctimas. (Nolasco Zavala; Izaguirre Chumpitaz; Cunyas Quispe; Diaz Aliaga; De la Cruz de fuertes; Roca Chuco y Sánchez Gutiérrez (2022) (ver Anexo 4)

En ese mismo orden de ideas la investigación realizada Aguilar (2019), considera que las actividades diarias han generado, que se logre exponer nuestra identidad y datos personales de manera digital, en muchas ocasiones las redes sociales han sido un medio esencial para que los ciberdelincuentes **hackeen** los datos personales, creen perfiles falsos y vulneren la información personal de sus víctimas y por consecuencia el robo de la identidad, por ello cuando se realiza un trámite bancario se brinda información personal el que tiene que ser corroborado con un documento oficial, el cual identifica a la persona, para evitar la usurpación y robo de identidad.

Por todo esta se concluye contrasta y corrobora el hackeo es el robo de información más usual, consiste que el delincuente vulnera correos, redes sociales (Facebook, Instagram y twitter) y cuentas bancarias, , para adquirir datos personales, y suplantar la identidad, lo más usual es vaciar las cuentas bancarias de sus víctimas. (Nolasco Zavala; Izaguirre Chumpitaz; Cunyas Quispe; Diaz Aliaga; De la Cruz de fuertes; Roca Chuco y Sánchez Gutiérrez (2022) (ver Anexo 4)

Con respecto al tercero objetivo específico: Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de **clonación tarjeta de crédito** por medios informáticos.

Con respecto a la tercera hipótesis específico: La ineficacia de la Ley N°30096, incide de forma negativa en el delito de **clonación tarjeta de crédito** por medios informáticos.

Respecto a la pregunta: ¿ha sido usted víctima del delito de clonación tarjeta de crédito a través de medios informáticos? podemos notar que la mayoría de los entrevistado no han sido víctima del delito de clonación de tarjeta de manera directa, pero, si un familiar o amigo cercano al entrevistado por ello y tiene conocimiento que en algunas ocasiones lograron vaciar las determinadas cuentas bancarias. Nolasco Zavala; Izaguirre Chumpitaz; Cunyas Quispe; Díaz Aliaga; de la cruz de fuertes; ; Roca Chuco; Benites Sapallanay ; Yarlequé Prieto; oliva Ávila y Sánchez Gutiérrez (2022) (ver Anexo 4)

Un resultado similar obtuvo Huayre (2021) donde señala los delincuentes tienen la libertad de aprovechar cualquier dispositivo con acceso a la tecnología para cometer actos delictivos cibernéticos; es por ello, que el presente trabajo de investigación tiene como objetivo Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos, asimismo indagar hasta qué punto la legislación presenta las iniciativas de políticas y técnicas que ayuden a batallar contra los delitos informáticos, coherentes con nuestra realidad peruana.

Así mismo en la presente investigación los entrevistado manifiestan que no han sido víctimas del delito de clonación de tarjeta de manera directa, pero si reciben correos maliciosos ,mensaje solicitando sus datos personales para luego clonar las tarjeta de débito y robar sus cuentas bancarias mediante el cambio de chip Nolasco Zavala; Izaguirre Chumpitaz; Cunyas Quispe; Díaz Aliaga; de la cruz de fuertes; ; Roca Chuco; Benites Sapallanay ; Yarlequé Prieto; oliva Ávila y Sánchez Gutiérrez (2022) (ver Anexo 4)

Resultado similar obtuvo Infante (2019) **donde** aborda un tema que considera relevante al avance y a la implementando de la tecnología informática, donde configura un panorama de aplicación y de posibilidades de juegos lícitos e ilícitos, donde se hace fundamental el derecho penal para regular los diversos

efectos de una situación nueva y de tantas potencialidades en el medio social; siendo los casos más notables, el hurto de la identidad virtual que frajelan a la sociedad, con lo cual se puede evidenciar, que no existe una correcta seguridad de los datos personales los correos, las redes sociales y las cuenta bancaria son vulnerados al formar parte de la tecnología informática; pues los datos personales son utilizado con fines ilícitos, produciendo un escena amplia de delitos de manera electrónica, es decir ilícitos digitales.

Sin embargo, Respecto a la pregunta: ¿Cree usted que su información o datos digitales está protegida cuando realizar una compra online? La mayoría de los entrevistados señalaron que prefieren realizar una compra de manera presencial puesto que al realizar una compra online no se sienten seguros y consideran que su información personal no está resguardada, las páginas web no presentan seguridad para el consumidor un ciberdelincuente puede elaborar la misma página web y cometer el ilícito penal Nolasco Zavala; Izaguirre Chumpitaz; Cunyas Quispe; Díaz Aliaga; de la cruz de fuertes; ; Roca Chuco; Benites Sapallanay ; Yarlequé Prieto; oliva Ávila y Sánchez Gutiérrez (2022) (ver Anexo 5)

Por todo esta se concluye contrasta y corrobora la clonación de tarjeta de débito es el robo de información más asiduo, consiste en duplicar la tarjeta solicitando un nuevo chip a la empresa telefónica y realizar la suplantación de identidad, para luego vaciar las cuentas bancarias de las víctimas, el no proporcionar la seguridad al consumidor genera que prefieran realizar una compra de manera física y no ser vulnerables a los ciberdelincuentes

Por ello Hernández (2009) hace hincapié en la seguridad informática como bien jurídico colectivo a tutelar, objeto de ataque con las conductas relacionadas a la cuestión informática. Se trata de un bien, cuya protección evita la lesión de una serie de bienes jurídicos de carácter individual puestos en peligro con tales conductas que atentan contra la seguridad de las redes y sistemas informático.

Asimismo lo entrevistados consideran que se debería implementar un presupuesto considerable en materiales digitales, capacitaciones y herramientas adecuadas de última generación para combatir la ciberdelincuencia la (**Divindat**) necesita un presupuesto adecuado para así ayudarse con implementos de última

generación contrarrestando la ciberdelincuencia Nolasco Zavala; Izaguirre Chumpitaz; Cunyas Quispe; Díaz Aliaga; de la cruz de fuertes; ; Roca Chuco; Benites Sapallanay ; Yarlequé Prieto; oliva Ávila y Sánchez Gutiérrez (2022) (ver Anexo 4)

Para concluir se reafirma y corrobora la hipótesis planteada en contraste con la teoría y estudios precedentes, en consecuencia, la suplantación de identidad por medios informáticos utiliza las diferentes técnicas como el phishing y el vishing para vulnerar la información personal de la víctima mediante correos maliciosos que aparentan ser fehacientes. Por ello, todo lo contrastado trabaja conjuntamente con el principio de primacía de la realidad, el cual es la puerta para salir de las apariencias y formalidades.

V. CONCLUSIONES

PRIMERO: Respecto del objetivo principal, se concluye que la ineficacia jurídica de la ley N°30096 tiene que ser regulada en los temas de transacciones comerciales como compra y venta por internet que realizan los delincuentes suplantando la identidad de sus víctimas.

SEGUNDO: Respecto del primer objetivo específico, se concluye que el phishing es una técnica de suplantación de identidad que tiene como finalidad engañar a los usuarios utilizando sistemas para que la víctima proporcione sus datos digitales,el PIN de la tarjeta de crédito u otros datos financieros. Normalmente cuando los suplantadores acceden a dicha información, la utilizan para robar dinero del usuario o usurpar su propiedad o su identidad.

TERCERO: Respecto del segundo objetivo específico, se concluye que los hackers utilizan diferentes métodos como el spyware que consiste en mantenerse oculto del usuario reclutando información, asimismo el ramsoware es un sistema que infecta y impide que se utilice la computadora, este virus afecto a usuarios vulnerando contraseñas bancarias, correos electrónicos y redes sociales, este método se utilizó mayormente para cometer ciberdelito.

CUARTO: Respecto del tercer objetivo específico, se concluye que la clonación de tarjeta de crédito o débito es uno de los principales fraudes financieros que en el tiempo de la pandemia han tomado mayor relevancia perjudicando a los usuarios, se ha podido verificar que las personas que cometen delitos informáticos son en la mayoría expertos en tecnología informática como también pueden ser novatos que se interesan por la tecnología.

Finalmente, los datos y contraseñas digitales deben ser considerados como un bien jurídico protegido, los que vulneran y transgreden la línea de la privacidad deben ser sancionados con penas privativas de la libertad.

VI. RECOMENDACIONES

1. Se recomienda que la Ley N°30096, a través de una iniciativa legislativa, regule las transacciones comerciales de compra y venta por internet. La razón de esta regulación se debe a que existen muchos casos la suplantación de identidad por transacciones comerciales mediante el uso del internet.

2. Se sugiere al usuario que cuando este reciba de manera sorpresiva correos maliciosos o spam donde le soliciten sus datos personales manifestando que usted se ganó la lotería o un carro de último modelo manifestando que para hacer valido dicho premio deberá abrir el correo electrónico y completar la información necesaria, para luego suplantar la identidad de la víctima y vaciar todas tus cuentas bancarias, por esta razón es mejor no responder el correo. Asimismo, se recomienda al usuario tener cuidado al navegar por internet, debido que en algunas ocasiones hay páginas web que contienen virus y buscan contaminar tu información, puesto que no se logra identificar al ciberdelincuente que se encuentra detrás de la pantalla propiciando un virus informático para sustraer la información personal.

3. Finalmente, el usuario debe tener cuidado al realizar un pago con tarjeta de crédito o débito, es mejor realizar una compra de manera presencial y con el dinero en físico, puesto que al realizar una compra online no se tiene la seguridad que la información proporcionada se encuentre protegido de los ciberdelincuentes, asimismo es necesario que Utilice clave de acceso, al mismo tiempo cambie la contraseña frecuentemente.

Recomendación es necesario investigar a profundidad sobre los hackers puesto que no se logró investigar a precisión el tema, asimismo, es necesario mencionar que los hackers son expertos en informática los cuales logran vulnerar cualquier red social, plataforma, aplicativo o sistema financiero, para cometer delitos que no se encuentren tipificados en la ley.

REFERENCIAS

Aguilar, E (2019). "*suplantación de la identidad digital con fines de trata de personas en Facebook".* (Publicación No 26092019). maestro en derecho de las tecnologías de la información y comunicación, infotec centro de investigación e innovación en tecnologías de la información y comunicación. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/363/1/INFOTEC_MDTIC_EAB_26092019.pdf

Alarcón, D., & Barrera, A. (2017) *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*. Universidad privada Norbert Wiener https://docplayer.es/88068396-Tesis-uso-de-internet-y-delitos-informaticos-en-los-estudiantes-de-primer-semestre-de-la-universidad-pedagogica-y-tecnologica-de.html

Acurio Del Pino, S. (2016). *Delitos informáticos: generalidades.* http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Aldecoa, M (2020) *El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019.* Tesis para obtener el título profesional de: ABOGADO. UNIVERSIDAD CESAR VALLEJO. file:///C:/Users/USER/Downloads/Aldecoa_JMR-SD%20-%20Utilizado%20Per%C3%BA.pdf

Bechara et. al, 2020 "*Análisis jurídico de la ley 1273 del 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos*". trabajo presentado para obtener el titulo de abogado. universidad cooperativa de Colombia http://www.knowledgecap.bigstarcreative.com/bitstream/20.500.12494/19788/3/2020_analisis_delitos_informaticos.pdf

Carriedo, L (2022). *"Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México*. Maestro en derecho de las tecnologías de información y comunicación. infotec centro de investigación e innovación en tecnologías de la información y comunicación https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/518/1/SOLUCIONESTRATEGICA_LMCT.pdf

Cavada Herrera, J. (2020). Cibercrimen y delito informático: definiciones en legislación internacional, nacional y extranjera. *Biblioteca del congreso nacional de chile BCN* (2014) volumen (1),1-8. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf

Chávez Suárez, G. R., & Palomino Mendiolaza, A. E. (2019). *Plan de negocio para combatir la obesidad en el distrito de Ate mediante un modelo de negocio "Crossfit"*. [Disertación de Maestría, Universidad San Ignacio de Loyola]. Universidad San Ignacio de Loyola. https://repositorio.usil.edu.pe/items/34499d43-3876-4d89-999f-2ad4f5231220

CITEC (2018) *Investigaciones cualitativas en ciencia y tecnología,* Primera edición abril 2018, Área de innovación y desarrollo S.L. https://books.google.com.pe/books?id=okdVDwAAQBAJ&lpg=PA1&dq=LIBROS%20DE%20METODOLOGIA%20DE%20INVESTIGACION%20CON%20EDITORIAL%20DEL%202012&hl=es&pg=PA26#v=onepage&q&f=false

Constitución Política del Perú, Art. 2, Inc. 2 (1993). C

Convenio de Budapest o Convenio sobre la Ciberdelincuencia aprobado el 2001

Código Penal. Decreto Legislativo N° 635, Art.207-B, 3 de abril de 1991 (Perú).

CONAPOC (2020) Diagnóstico Situacional Multisectorial sobre la Ciberdelincuencia en el Perú. Primera edición digital, diciembre 2020. Ministerio de Justicia y Derechos Humanos Observatorio Nacional de Política Criminal Calle Scipión Llona 350, Miraflores file:///C:/Users/20210/Downloads/Diagn%C3%B3stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20%20en%20el%20Per%C3%BA%20(1).pdf

Chiluisa, D. (2021). *Los delitos informáticos y los vacíos legales que afectan a los ciudadanos.* Trabajo de titulación previo a la obtención del título de Abogado de los tribunales y juzgados de la república del Ecuador. Universidad católica de Santiago de guayaquil http://repositorio.ucsg.edu.ec/bitstream/3317/16501/1/T-UCSG-PRE-JUR-DER-MD-334.pdf

Chigirev, Alexey. (2021). *Plan de negocios sobre monitoreo de empleados en el marco del teletrabajo.* Pontificia Universidad Católica Argentina. https://repositorio.uca.edu.ar/bitstream/123456789/11987/1/plan-negocios-monitoreo-empleados.pdf

ferro, J (2020) *Informática forense, la paz murillo, (2020).* 1era edicion octubre 2020 https://books.google.com.pe/books?id=NO7JDwAAQBAJ&pg=PA9&dq=delitos+inform%C3%A1ticos+suplantacion+de+identidad&hl=es-419&sa=X&ved=2ahUKEwjvv-Lkxq_8AhUAHrkGHUBXBUsQ6AF6BAgGEAI#v=onepage&q=delitos%20inform%C3%A1ticos%20suplantacion%20de%20identidad&f=false

Grenni & Fernandez (2018) *Cibercrimen y delitos informáticos los nuevos tipos penales en la era de internet* / compilado por Ricardo Antonio Parada ; José Daniel Errecaborde. - 1a ed . - Ciudad Autónoma de Buenos AIRES: Erreius, 2018. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963

Huamán, M. (2020) *Los delitos informáticos en Perú y la suscripción del convenio de Budapest*. Tesis para optar el título profesional de abogada. universidad andina de cusco.https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y

Huayre, I.(2021). E*l impacto del cibercrimen en delitos de estafa en el Distrito de Lima, 2021.* para optar el título profesional en derecho. universidad peruana de las américas.http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1729/TRABAJO%20DE%20INVESTIGACI%C3%93N%20%281%29.pdf?sequence=1&isAllowed=y

Hernández, L. (2009) *El delito informático.* Eguzkilore volumen (23) ,227 – 243 https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Infante, B. (2019).*"análisis del delito de hurto de identidad virtual: frente a la seguridad de los sistemas informáticos".* Para optar el título profesional de abogada. universidad nacional de Piura. https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/2524/DECP-INF-GUE-2019.pdf?sequence=1&isAllowed=y

Loredo González, J, & Ramírez Granados, A. (2013). *Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo.* Celerinet , 44–51. http://eprints.uanl.mx/3536/

Leyva Serrano, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris et Investigatio* , *1* , 29–47. https://doi.org/10.15381/lucerna.v0i1.18373

Ley N° 30096 .Ley de delitos informáticos Art. 9 (21 de octubre del 2013).

Ley N° 3017. Ley que modifica la *Ley* 30096 de Delitos Informáticos. (10 de marzo de 2014)

Martins, B. (2022). *Convenio de Budapest sobre la Ciberdelincuencia en América Latina* . derechosdigitales.org. https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

Mori, F. (2019).*"Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de lima, periodo 2008 al 2012"* Tesis para optar el grado académico de: maestro en derecho penal. UNIVERSIDAD FEDERICO VILLAREAL. f https://1library.co/document/q7lrlxoy-delitos-informaticos-proteccion-penal-intimidad-distrito-judicial-periodo.html

Montaperto, J.(2018). "Suplantación de Identidad: Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino". (Tesis de Grado). Universidad Siglo 21, Argentina. https://www.pensamientopenal.com.ar/doctrina/90107-suplantacion-identidad-analisis-sobre-su-falta-regulacion-ordenamiento-juridico

MONJA, G.(2022) Delitos informáticos en las entidades bancarias -suplantación de identidad. Para optar el título profesional de abogado. Universidad Peruana de las Américas http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1953/TRABAJO%20DE%20INVES.MONJA%20ESQUIVEL%2c%20GIULIANA%20MARINA.pdf?sequence=1&isAllowed=y

Martínez, M.(2018). *Cibercrimen y delitos informáticos los nuevos tipos penales en la era de internet* / compilado por Ricardo Antonio Parada ; José Daniel Errecaborde. - 1a ed . - Ciudad Autónoma de Buenos AIRES: Erreius, 2018. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963

OFAEC.(2021). *Ciberdelincuencia en el Perú: Pautas para una investigación fiscal especializada oficina de análisis estratégico contra la criminalidad.* Foto de portada: Freepik https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20P

Quintero de Sola, R (2021*) Delito Informático. volumen* (1), 1-25 https://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf

Romero et. al,(2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades* . Editorial Científica 3Ciencias. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Ramos, J.(2022*). Cómo protegerte del phishing:* Evita que te roben tu información y tu dinero. copyright ISBN: 9783987623295 verlag GD publishing LTd.&CoKG,Belin https://books.google.com.pe/books?id=0kaFEAAAQBAJ&pg=PT2&lpg=PT2&dq=C%C3%B3mo+protegerte+del+phishing:+Evita+que+te+roben+tu+informaci%C3%B3n+y+tu+dinero+Por+Juanjo+Ramos&source=bl&ots=MNbZQi0qrM&sig=ACfU3U3wnRazBQOyr6DQXl4G7XhxtxY_QA&hl=es-419&sa=X&ved=2ahUKEwi295GTzq_8AhXeA7kGHYiSAMIQ6AF6BAgfEAM#v=onepage&q=C%C3%B3mo%20protegerte%20del%20phishing%3A%20Evita%20que%20te%20roben%20tu%20informaci%C3%B3n%20y%20tu%20dinero%20Por%20Juanjo%20Ramos&f=false

Sain, G.(2018). *Cibercrimen y delitos informáticos los nuevos tipos penales en la era de internet* / compilado por Ricardo Antonio Parada ; José Daniel Errecaborde. - 1a ed . - Ciudad Autónoma de Buenos AIRES: Erreius, 2018. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963

Sánchez J. (2016). Manual autos instructivos delitos informático. https://es.scribd.com/document/375488335/Curso-Delitos-Informaticos-Jhon-Sanchez-Chirinos-2016

Santos, M. (2020). Análisis de los medios probatorios idóneos para comprobar los delitos electrónicos en el Distrito Nacional, año 2019. Maestría en Derecho Penal y Procesal Penal. universidad apec

https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_06_2020_ET210180.pdf

Temperini, M.(2018). *Cibercrimen y delitos informáticos los nuevos tipos penales en la era de internet* / compilado por Ricardo Antonio Parada ; José Daniel Errecaborde. - 1a ed . - Ciudad Autónoma de Buenos AIRES: Erreius, 2018. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963

ANEXOS

ANEXO 1

CARTA DE PRESENTACIÓN DEL INSTRUMENTO PARA VALIDACIÓN

Sr. (a) **ALBERTO REYMONDI ANGELES MACAVILCA**
Previo cordial saludo,

El presente es para informarle, que estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener el título de abogado.
Por lo tanto, me es grato dirigirme hacia su persona, e invitarlo(a) a validar el instrumento, puesto que es de suma importancia obtener su validación como experto, para la continuidad y fiabilidad de la investigación.
Asimismo, se agradece el tiempo y el apoyo brindado.

ATENTAMENTE
Quispe Ayala, Victor Faustino
Quispe Saire, Laura Sofia

CARTA DE PRESENTACIÓN DEL INSTRUMENTO PARA VALIDACIÓN

Sr. (a) **ALEXANDER SOLORZANO PALOMINIO**

Previo cordial saludo,

El presente es para informarle, que estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener el título de abogado.

Por lo tanto, me es grato dirigirme hacia su persona, e invitarlo(a) a validar el instrumento, puesto que es de suma importancia obtener su validación como experto, para la continuidad y fiabilidad de la investigación.

Asimismo, se agradece el tiempo y el apoyo brindado.

ATENTAMENTE

Quispe Ayala, Victor Faustino

Quispe Saire, Laura Sofia

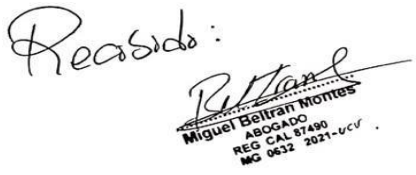
CARTA DE PRESENTACIÓN DEL INSTRUMENTO PARA VALIDACIÓN

Sr. (a) **MIGUEL BELTRAN MONTES**
Previo cordial saludo,

El presente es para informarle, que estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener el título de abogado.

Por lo tanto, me es grato dirigirme hacia su persona, e invitarlo(a) a validar el instrumento, puesto que es de suma importancia obtener su validación como experto, para la continuidad y fiabilidad de la investigación.

Asimismo, se agradece el tiempo y el apoyo brindado.



ATENTAMENTE
Quispe Ayala, Victor Faustino
Quispe Saire, Laura Sofia

CARTA DE PRESENTACIÓN DEL INSTRUMENTO PARA VALIDACIÓN

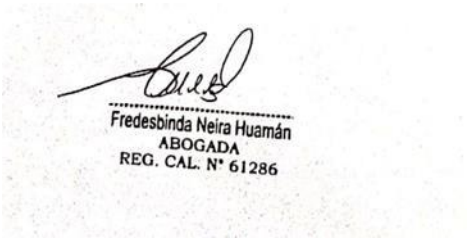
Sr. (a) **FREDESBINDA NEIRA HUAMÁN** CAL N° 61286

Previo cordial saludo,

El presente es para informarle, que estamos realizando un estudio de ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS para obtener el título de abogado.

Por lo tanto, me es grato dirigirme hacia su persona, e invitarlo(a) a validar el instrumento, puesto que es de suma importancia obtener su validación como experto, para la continuidad y fiabilidad de la investigación.

Asimismo, se agradece el tiempo y el apoyo brindado.



ATENTAMENTE

Quispe Ayala, Victor Faustino

Quispe Saire, Laura Sofia

CARTA DE PRESENTACIÓN DEL INSTRUMENTO PARA VALIDACIÓN

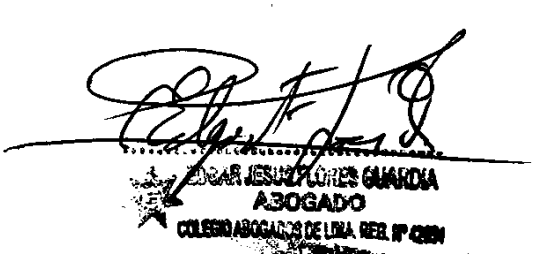
Sr. (a) **EDGAR JESÚS FLORES GUARDIA** CAL° 42654

Previo cordial saludo,

El presente es para informarle, que estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por lo tanto, me es grato dirigirme hacia su persona, e invitarlo(a) a validar el instrumento, puesto que es de suma importancia obtener su validación como experto, para la continuidad y fiabilidad de la investigación.

Asimismo, se agradece el tiempo y el apoyo brindado.



ATENTAMENTE

Quispe Ayala, Victor Faustino

Quispe Saire, Laura Sofia

CARTA DE PRESENTACIÓN DEL INSTRUMENTO PARA VALIDACIÓN

Sr. (a) **EDWIN FLORES CASTILLÓN** CAP N° 2146

Previo cordial saludo,

El presente es para informarle, que estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por lo tanto, me es grato dirigirme hacia su persona, e invitarlo(a) a validar el instrumento, puesto que es de suma importancia obtener su validación como experto, para la continuidad y fiabilidad de la investigación.

Asimismo, se agradece el tiempo y el apoyo brindado.

ATENTAMENTE

Quispe Ayala, Victor Faustino

Quispe Saire, Laura Sofia

ANEXO 2

Anexo E1

Matriz de validez de los Ítems de la Entrevista a Profundidad por Expertos.

Apellido y Nombre del Experto:	Profesión	Nombre del Instrumento:	Autor del instrumento:
ALBERTO RAYMUNDO ANGELES MACAVILCA	ABOGADO Firma	Valoración de los Ítems del instrumento	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia

Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1				✓	
2				✓	
3				✓	
4				✓	
5				✓	
6				✓	
7				✓	
8				✓	
9				✓	
10				✓	
11				✓	
12				✓	

Nota: Adaptado de "Validez de instrumento de investigación", por Solís, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

Anexo C1

Matriz de Validez de un instrumento de Investigación

Apellido y Nombre del Experto:	Profesión	Nombre del Instrumento:	Autor del instrumento:
ALBERTO REYNOLDI ANGELES MACAYLLA	ABOGADO Firma	Instrumento de evaluación para determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia

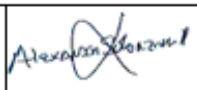
Criterios		Valoración		Observación
		SI	NO	
1. Claridad	Esta formado con el lenguaje claro y apropiado.	✓		
2. Objetividad	Esta expresado en conductas observables.	✓		
3. Pertinencia	Adecuado al avance de la ciencia pedagógica.	✓		
4. Organización	Existe una organización lógica.	✓		
5. Suficiencia	Comprende los aspectos en calidad y cantidad.	✓		
6. Adecuación	Adecuado para valorar el constructo o variable a medir.	✓		
7. Consistencia	Basado en aspectos teóricos- científicos.	✓		
8. Coherencia	Entre las definiciones, dimensiones e indicadores.	✓		
9. Metodología	La estrategia responde al propósito de la medición.	✓		
10. Significatividad	Es útil y adecuado para la investigación.	✓		

Nota: Adaptado de "Validez de instrumento de investigación", por Solís,, C., 2020, Material académico del curso Estadistica aplicada a la investigación, Universidad Continental, Huancayo .

ALBERTO REYNOLDI ANGELES MACAYLLA
ABOGADO
REG. CAL. N° 68196

Anexo E2

Matriz de validez de los Ítems de la Entrevista a Profundidad por Expertos.

Apellido y Nombre del Experto:	Profesión	Nombre del Instrumento:	Autor del instrumento:
SOLORZANO PALOMINO ALEXANDER	ABOGADO Firma 	Valoración de los Ítems del instrumento	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia

Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1			X		
2			X		
3			X		
4			X		
5			X		
6			X		
7				X	
8				X	
9			X		
10				X	
11				X	
12				X	

Nota: Adaptado de "Validez de instrumento de investigación", por Solís, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

Anexo C2

Matriz de Valides de un instrumento de Investigación

Apellido y Nombre del Experto:		Profesión		Nombre del Instrumento:		Autor del instrumento:
ALEXANDER SOLORZANO PALOMINIO		ABOGADO		Instrumento de evaluación para determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.		Quispe Ayala Victor Faustino Quispe Saire Lura Sofia
		Firma				
Criterios				Valoración		Observación
				SI	NO	
1.	Claridad	Esta formado con el lenguaje claro y apropiado		X		
2.	Objetividad	Esta expresado en conductas observables		X		
3.	Pertinencia	Adecuado al avance de la ciencia pedagógica		X		
4.	Organización	Existe una organización lógica		X		
5.	Suficiencia	Comprende los aspectos en calidad y cantidad		X		
6.	Adecuación	Adecuado para valorar el constructo o variable a medir		X		
7.	Consistencia	Basado en aspectos teóricos- científicos.		X		
8.	Coherencia	Entre las definiciones, dimensiones e indicadores-		X		
9.	Metodología	La estrategia responde al propósito de la medición		X		
10.	Significatividad	Es útil y adecuado para la investigación		X		

Nota: Adaptado de "Validez de instrumento de investigación" , por Solis, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

Anexo E3

Matriz de validez de los Ítems de la Entrevista a Profundidad por Expertos.

Apellido y Nombre del Experto:	Profesión		Nombre del Instrumento:	Autor del instrumento:
Beltran Montes Miguel	Abogado		Valoración de los Ítems del instrumento	Quispe Ayala Victor Faustino
	Firma	Beltrans		Quispe Saire Lura Sofia

Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1				X	
2				X	
3				X	
4				X	
5				X	
6				X	
7				X	
8				X	
9				X	
10				X	
11				X	
12				X	

Nota: Adaptado de "Validez de instrumento de investigación", por Solís, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

Miguel Beltran Montes
ABOGADO
REG CAL 87490
MG 0432 2021-UCU

Anexo C3

Matriz de Validez de un instrumento de Investigación

Apellido y Nombre del Experto:	Profesión	Nombre del Instrumento:	Autor del instrumento:
Beltran Montes Miguel	Abogado Firma	Instrumento de evaluación para determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia

	Criterios	Valoración		Observación
		SI	NO	
1. Claridad	Esta formado con el lenguaje claro y apropiado.	Si		—
2. Objetividad	Esta expresado en conductas observables.	Si		—
3. Pertinencia	Adecuado al avance de la ciencia pedagógica.	Si		—
4. Organización	Existe una organización lógica.	Si		—
5. Suficiencia	Comprende los aspectos en calidad y cantidad.	Si		—
6. Adecuación	Adecuado para valorar el constructo o variable a medir.	Si		—
7. Consistencia	Basado en aspectos teóricos- científicos.	Si		—
8. Coherencia	Entre las definiciones, dimensiones e indicadores.	Si		—
9. Metodología	La estrategia responde al propósito de la medición.	Si		—
10. Significatividad	Es útil y adecuado para la investigación.	Si		—

Nota: Adaptado de "Validez de instrumento de investigación", por Solís,. C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo .

Miguel Beltran Montes
ABOGADO
REG CAL 87490
ICG 0432 2021

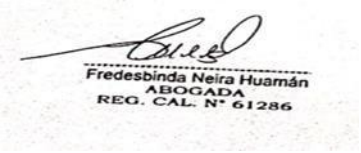
Anexo E4

Matriz de validez de los Ítems de la Entrevista a Profundidad por Expertos.

Apellido y Nombre del Experto:	Profesión		Nombre del Instrumento:	Autor del instrumento:
FREDESBINDA NEIRA HUAMÁN	Abogada		Valoración de los Ítems del instrumento	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia
	Firma			

Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1			X		
2			X		
3			X		
4			X		
5			X		
6			X		
7		X			
8				X	
9				X	
10			X		
11				X	
12				X	

Nota: Adaptado de "Validez de instrumento de investigación", por Solis, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.



Anexo C4

Matriz de Validez de un instrumento de Investigación

Apellido y Nombre del Experto:	Profesión	Nombre del Instrumento:	Autor del instrumento:
FREDESBINDA NEIRA HUAMÁN	Abogada Firma	Instrumento de evaluación para determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia

Criterios		Valoración		Observación
		SI	NO	
1. Claridad	Esta formado con el lenguaje claro y apropiado.	X		
2. Objetividad	Esta expresado en conductas observables.	X		
3. Pertinencia	Adecuado al avance de la ciencia pedagógica.	X		
4. Organización	Existe una organización lógica.	X		Los operadores de justicia no dan cumplimiento a la norma.
5. Suficiencia	Comprende los aspectos en calidad y cantidad.	X		
6. Adecuación	Adecuado para valorar el constructo o variable a medir.	X		
7. Consistencia	Basado en aspectos teóricos- científicos.	X		Científico, no .
8. Coherencia	Entre las definiciones, dimensiones e indicadores.	X		
9. Metodología	La estrategia responde al propósito de la medición.	X		
10. Significatividad	Es útil y adecuado para la investigación.	X		

Fredesbinda Neira Huamán
ABOGADA
REG. CAL. N° 61286

Nota: Adaptado de "Validez de instrumento de investigación", por Solis, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

Anexo E5

Matriz de validez de los Ítems de la Entrevista a Profundidad por Expertos.

Apellido y Nombre del Experto:	Profesión	Nombre del Instrumento:	Autor del instrumento:
FLORES GUARDIA, EDGAR JESÚS	ABOGADO Firma	Valoración de los Ítems del instrumento	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia

Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1				X	
2				X	
3		X			
4			X		
5				X	
6			X		
7				X	
8				X	
9		X			
10				X	
11			X		
12				X	

Nota: Adaptado de "Validez de instrumento de investigación", por Solis, C., 2020, Material académico del curso Estadistica aplicada a la investigación, Universidad Continental, Huancayo.

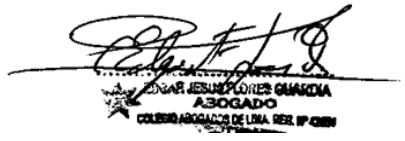
EDGAR JESUS FLORES GUARDIA
ABOGADO
COLEGIO ABOGADOS DE LIMA REG. N° 43884

Anexo C5

Matriz de Validez de un instrumento de Investigación

Apellido y Nombre del Experto:	Profesión	Nombre del Instrumento:	Autor del instrumento:
FLORES GUARDIA, EDGAR JESÚS	ABOGADO Firma  Edgar Jesús Flores Guardia	Instrumento de evaluación para determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.	Quispe Ayala Victor Faustino Quispe Saire Laura Sofia

Criterios		Valoración		Observación
		SI	NO	
1. Claridad	Esta formado con el lenguaje claro y apropiado.	X		
2. Objetividad	Esta expresado en conductas observables.	X		
3. Pertinencia	Adecuado al avance de la ciencia pedagógica.	X		
4. Organización	Existe una organización lógica.	X		
5. Suficiencia	Comprende los aspectos en calidad y cantidad.	X		
6. Adecuación	Adecuado para valorar el constructo o variable a medir.	X		
7. Consistencia	Basado en aspectos teóricos- científicos.	X		
8. Coherencia	Entre las definiciones, dimensiones e indicadores.	X		Respecto al tercer objetivo especifico, debería ser tarjeta de debito no crédito.
9. Metodología	La estrategia responde al propósito de la medición.	X		
10. Significatividad	Es útil y adecuado para la investigación.	X		



Nota: Adaptado de "Validez de instrumento de investigación", por Solís, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

Anexo E6

Matriz de validez de los Ítems de la Entrevista a Profundidad por Expertos.

Apellido y Nombre del Experto:		Profesión		Nombre del Instrumento:	Autor del instrumento:
EDWIN FLORES CASTILLON		DR. ABOGADO		Valoración de los Ítems del instrumento	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia
		Firma			
Ítems	Valoración				Descripción
	Deficiente (0)	Regular (1)	Bueno (2)	Excelente (3)	
1				X	
2			X		
3				X	
4				X	
5				X	
6				X	
7				X	
8				X	
9				X	
10				X	
11				X	
12				X	

Nota: Adaptado de "Validez de instrumento de investigación", por Solís, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

Doctor en Derecho
Edwin Flores Castillon
ABOGADO
CAP. 2145

Anexo C6

Matriz de Validez de un instrumento de Investigación

Apellido y Nombre del Experto:	Profesión	Nombre del Instrumento:	Autor del instrumento:
EDWIN FLORES CASTILLON	ABOGADO Firma	Instrumento de evaluación para determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos.	Quispe Ayala Victor Faustino Quispe Saire Lura Sofia

Criterios		Valoración		Observación
		SI	NO	
1. Claridad	Esta formado con el lenguaje claro y apropiado.	X		
2. Objetividad	Esta expresado en conductas observables.	X		
3. Pertinencia	Adecuado al avance de la ciencia pedagógica.	X		
4. Organización	Existe una organización lógica.	X		
5. Suficiencia	Comprende los aspectos en calidad y cantidad.	X		
6. Adecuación	Adecuado para valorar el constructo o variable a medir.	X		
7. Consistencia	Basado en aspectos teóricos- científicos.	X		
8. Coherencia	Entre las definiciones, dimensiones e indicadores.	X		
9. Metodología	La estrategia responde al propósito de la medición.	X		
10. Significatividad	Es útil y adecuado para la investigación.	X		

Nota: Adaptado de "Validez de instrumento de investigación", por Solís, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo .

ANEXO 4

ENTREVISTA 001

Entrevistador: Quispe Saire Laura Sofia Fecha: 15 / 10 /2022

Entrevistado: YVONNE CAROLINA CUNYAS QUISPE

Introducción

Buenos dias , mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 21:47 hrs del 15 de octubre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones.

Para agilizar la toma de informacion, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podria perder cuestiones importantes . Asimismo le reordamos que la informacion es estrictamente confidencial ;por ende todo lo recabado sera de indole academico .

Ante ello,¿existe algun inconveniente en que grabemos la conversacion ?

Respuestas del entrevistado : (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas:

ENTREVISTA 002

Entrevistador: Quispe Saire Laura Sofia **Fecha: 20 / 10 /2022**

Entrevistado: JULIO CESAR SANCHEZ GUTIERREZ

Introducción

Buenos días, mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 17:40 hrs del 20 de octubre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones. Para agilizar la toma de información, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podría perder cuestiones importantes. Asimismo, le reordamos que la informacion es estrictamente confidencial por ende todo lo recabado será de índole académico.

Ante ello, ¿existe algun inconveniente en que grabemos la conversación?

Respuestas del entrevistado: (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas:

ENTREVISTA 003

Entrevistador: Quispe Saire Laura Sofia **Fecha: 21 / 10 /2022**

Entrevistado: MARIA TERESA DE LA CRUZ DE FUERTES

Introducción

Buenos dias, mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 20:40 hrs del 21 de octubre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones. Para agilizar la toma de información, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podría perder cuestiones importantes. Asimismo, le reordamos que la informacion es estrictamente confidencial por ende todo lo recabado sera de indole académico.

Ante ello, ¿existe algún inconveniente en que grabemos la conversación?

Respuestas del entrevistado: (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas:

ENTREVISTA 004

Entrevistador: Quispe Saire Laura Sofia Fecha: 23 / 10 /2022

Entrevistado: FRANK IZAGUIRRE CHUMPITAZ - CAL 84167

Introducción

Buenos días, mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 17:00 hrs del 23 de octubre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones.

Para agilizar la toma de informacion, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podria perder cuestiones importantes . Asimismo le reordamos que la informacion es estrictamente confidencial por ende todo lo recabado sera de indole academico .

Ante ello,¿existe algun inconveniente en que grabemos la conversacion ?

Respuestas del entrevistado : (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas:

FRANK ANTONY
IZAGUIRRE CHUMPITAZ
ABOGADO
Reg. 84167

ENTREVISTA 005

Entrevistador: Quispe Saire Laura Sofia **Fecha: 23 / 10 /2022**

Entrevistado: José Luis Nolasco Zavala

<u>Introducción</u>

Buenos dias , mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 18:00 hrs del 23 de octubre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones. Para agilizar la toma de información, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podría perder cuestiones importantes. Asimismo, le reordamos que la informacion es estrictamente confidencial por ende todo lo recabado será de índole académico.

Ante ello, ¿existe algún inconveniente en que grabemos la conversacion?

Respuestas del entrevistado: (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas:

ENTREVISTA 006

Entrevistador: Quispe Saire Laura Sofia Fecha: 07/ 11 /2022

Entrevistado: MELISSA NÉLIDA ROCA CHUCO

Introducción

Buenos días, mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 21:51 hrs del 07 de noviembre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones. Para agilizar la toma de información, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podría perder cuestiones importantes. Asimismo, le reordamos que la informacion es estrictamente confidencial por ende todo lo recabado será de índole académico.

Ante ello, ¿existe algún inconveniente en que grabemos la conversación?

Respuestas del entrevistado: (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas

ENTREVISTA 007

Entrevistador: Quispe Saire Laura Sofia **Fecha: 08/ 11 /2022**

Entrevistado: DEISE DIAZ ALIAGA **CAL 67515**

Introducción

Buenos días, mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 21:19 hrs del 08 de noviembre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones. Para agilizar la toma de informacion, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podria perder cuestiones importantes . Asimismo le reordamos que la informacion es estrictamente confidencial por ende todo lo recabado sera de indole academico .

Ante ello,¿existe algun inconveniente en que grabemos la conversacion ?

Respuestas del entrevistado : (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas:

ENTREVISTA 008

Entrevistador: Quispe Saire Laura Sofia Fecha: 08/ 12 /2022

Entrevistado: PEPE BENITES SAPALLANAY

Introducción

Buenos días, mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

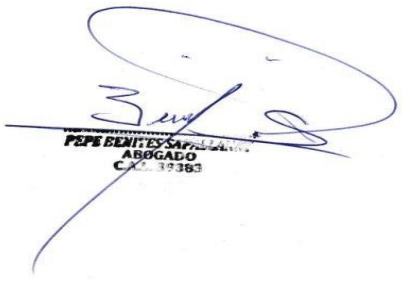
Por tal motivo, siendo las 17:25 hrs del 08 de diciembre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones. Para agilizar la toma de información, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podría perder cuestiones importantes. Asimismo, le reordamos que la informacion es estrictamente confidencial por ende todo lo recabado será de índole académico.

Ante ello, ¿existe algún inconveniente en que grabemos la conversación?

Respuestas del entrevistado: (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas:



ENTREVISTA 009

Entrevistador: Quispe Saire Laura Sofia **Fecha: 22/ 12/2022**

Entrevistado: Pilar Yarlequé Prieto **CAL: 50089**

Introducción

Buenos dias , mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 20:35 hrs del 22 de diciembre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones.

Para agilizar la toma de informacion, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podria perder cuestiones importantes . Asimismo le reordamos que la informacion es estrictamente confidencial por ende todo lo recabado sera de indole academico .

Ante ello,¿existe algun inconveniente en que grabemos la conversacion ?

Respuestas del entrevistado : (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas :

T. PILAR YARLEQUÉ PRIETO
ABOGADO
C.A.L. 50089

ENTREVISTA 010

Entrevistador: Quispe Saire Laura Sofia Fecha: 28 / 12 /2022

Entrevistado: DR. JUAN ANTONIO OLIVA AVILA CAL 26560 CASILLA ELE:61865

Introducción

Buenos días, mi nombre es Quispe Saire, Laura Sofia y junto a mi compañero Quispe Ayala, Victor Faustino estamos realizando un estudio de **ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS** para obtener nuestro título de abogado.

Por tal motivo, siendo las 08:38 hrs del 28 de diciembre 2022 realizamos una entrevista semiestructurada, asimismo se agradece el tiempo brindado. En este sentido, siéntase libre de compartir sus ideas. Aquí no hay respuestas correctas e incorrectas, lo que importa es su opinión sincera, ya que la información que usted nos otorgue será únicamente materia de investigación, al igual que otras opiniones. Para agilizar la toma de informacion, resulta mucha utilidad grabar la conversacion. Tomar notas a mano, demoraria y se podria perder cuestiones importantes . Asimismo, le recordamos que la informacion es estrictamente confidencial por ende todo lo recabado sera de indole académico.

Ante ello, ¿existe algun inconveniente en que grabemos la conversación?

Respuestas del entrevistado : (SI/NO).

Desde ya, ¡muchas gracias!

Por lo cual hemos formulado las siguientes preguntas:

INSTRUMENTO DE RECOLECCION DE

DATOS GUÍAS DE ENTREVISTAS

TÍTULO

ANÁLISIS JURÍDICO DE LA INEFICACIA DE LA LEY N°30096 EN EL DELITO DE SUPLANTACIÓN DE IDENTIDAD POR MEDIOS INFORMÁTICOS.

OBJETIVO GENERAL

Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos

Pregunta:

1. ¿Considera usted que existen vacíos legales en la Ley N° 30096, Ley de delitos informáticos, ¿respecto a la suplantación de identidad?
2. En su opinión, ¿Cree usted que la suscripción del convenio de Budapest ha garantizado la protección de la Ley N° 30096, Ley de delitos informáticos?
3. ¿Considera usted que las fiscalías especializadas de delitos informáticos en materia de cibercriminalidad, poseen herramientas digitales pertinentes a la suplantación de identidad de la víctima?
4. ¿Conoce usted los delitos informáticos más asiduos en el Perú? ¿La suplantación de identidad conocido como el pshing que se está empleando en la actualidad, tenemos los fraudes informáticos que es otro de los delitos que regula la Ley N°30096?

PRIMER OBJETIVO ESPECÍFICO

Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito del Phishing por medios informáticos.

Pregunta:

5. ¿Considera usted que la ineficacia de la Ley N°30096 en el delito del Phishing, se configura a través de medios informáticos?
6. ¿Conoce usted la técnica del phishing que utilizan los ciberdelincuentes para obtener información personal de sus víctimas?
7. ¿Considera usted que la difusión de contenido engañoso en las redes sociales, SMS o llamadas telefónicas, coadyuva la suplantación de identidad con la modalidad del Vishing?

SEGUNDO OBJETIVO ESPECÍFICO

Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito realizado por un Hacker por medios informáticos.

Pregunta:

8. ¿Conoce usted las técnicas que utilizan los hackers para vulnerar los datos personales o información digital, utilizando la tecnología informática?
9. ¿Considera usted que los operadores de las fiscalías especializadas en delitos informáticos en materia de cibercriminalidad son eficientes en el ejercicio de sus funciones?
10. En su opinión, ¿Cree usted que los operadores de la fiscalía deberían estar en constante capacitación?

TERCERO OBJETIVO ESPECÍFICO

Determinar la manera en la que incide la ineficacia de la Ley N°30096 en el delito de clonación tarjeta de débito por medios informáticos.

Pregunta:

11. En su opinión ¿ha sido usted víctima del delito de clonación tarjeta de crédito a través de medios informáticos?
12. En su opinión, ¿Cree usted que su información o datos digitales está protegida cuando realizar una compra online?

.

ANEXO 3

Tabla 10

Matriz del consolidado de la Validez de un Instrumento de Investigación - Entrevistas a Profundidad

Criterios	Descripción	Expertos						Suma de acuerdos Total (S)	V Aiken	Descripción
		E1	E2	E3	E4	E5	E6			
1. Claridad	Está formado con el lenguaje claro y apropiado.	1	1	1	1	1	1	6	1.00	**Fuerte**
2. Objetividad	Está expresado en conductas observables.	1	1	1	1	1	1	6	1.00	**Fuerte**
3. Pertinencia	Adecuado al avance de la ciencia pedagógica.	1	1	1	1	1	1	6	1.00	**Fuerte**
4. Organización	Existe una organización lógica.	1	1	1	1	1	1	6	1.00	**Fuerte**
5. Suficiencia	Comprende los aspectos en calidad y cantidad.	1	1	1	1	1	1	6	1.00	**Fuerte**
6. Adecuación	Adecuado para valorar el constructo o variable a medir.	1	1	1	1	1	1	6	1.00	**Fuerte**
7. Consistencia	Basado en aspectos teórico-científicos	1	1	1	1	1	1	6	1.00	**Fuerte**
8. Coherencia	Entre las definiciones, dimensiones e indicadores.	1	1	1	1	1	1	6	1.00	**Fuerte**
9. Metodología	La estrategia responde al propósito de la medición	1	1	1	1	1	1	6	1.00	**Fuerte**
10. Significatividad	Es útil y adecuado para la investigación.	1	1	1	1	1	1	6	1.00	**Fuerte**

Nota: Adaptado de “Validez de instrumentos de investigación”, por Solís, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

ANEXO 4

Tabla 11

Matriz de recopilación de respuestas de los entrevistados

Preguntas /Entrevistado	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
P1	• Si • Debería ser más explicito	• Si • No se encuentra tipificado	• Si	• Si • No sanciona el delito propiamente.	• SI • No se encuentra establecido	• No señala las técnicas que utiliza el ciberdelincuente	• No especifica las los métodos que se utilizan	• No presenta las técnicas que utiliza el ciberdelincuente	• No señala las diferentes técnicas del ciberdelincuente	• Si especifica siempre que esté en la ley
P2	• Si • Debería adecuar a legislación peruana	• Si • Adecuarse a la legislación peruana	• Si • Tendría que adecuarse a la realidad	• Si • Permite poder adecuarse al CPP	• Si • Debería adecuarse a la realidad peruana	• Si • Es un convenio entre países	• Permite adecuarse la comunidad europea	• Permite incrementar una cooperación internacional	• Permite gestionar requerimientos internacionales	• Permite enlaces entre países
P3	• Si • Carece de herramientas	• Si • Carece de tecnología	• No • Carece de implementación tecnológica	• Si • No utiliza los medios logísticos	• Si • Implementar la tecnología	• No • Carece de herramientas	• No • Carece de técnicas y del tic	• No • Carece de un presupuesto adecuado	• Carece de tecnología cibernética	• Carece de tecnología
P4	• Si • Fraude informático	• Suplantación de identidad	• Fraude informático	• Si • Suplantación de identidad	• Si • Suplantación de identidad	• Pornografía infantil • Suplantación de identidad	• Suplantación identidad y fraude informático	• Fraude informático	• Fraude informático	• Suplantación de identidad

Preguntas /Entrevistado	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
P5	• Si • Hurto cibernético	• Si • Clonación de tarjeta	• Si	• Si • Mediante el internet	• Si • Robo cibernético	• Si • Es un mecanismo de robo de información	• Si • Buscan utilizar la información personal	• Mecanismo que utiliza el ciberdelincuente	• Utilizan datos personales	• Utilizan herramientas digitales
P6	• Si • Mediante correos electrónicos	• SI • Correos maliciosos	• Si • Correos	• Si • Por Páginas web, los cookis y keyloyer	• Si • Correos electrónicos	• Mensajes, correos paginas web	• Si mediante los correos o llamadas	• Mediante Sms, llamadas y correos	• Utilizan llamadas y correos electrónicos	• Mediante llamadas
P7	• Si • Utilizan instituciones financieras	• Si • Mediante llamadas telefónica	• Si • Llamadas	• Si • Por llamadas y SMS	• Si • Utilizan premios para captar a su victima	• Si • Mediante contenido engañoso	• Si, no hay un ente regulador.	• Deberían garantizar la protección información	• Utilizan llamada telefónicas y correos	• Utilizan informacion falsa
P8	• Si • Vulneran datos personales	• Si • Utilizan las redes	• Si • Utilizan software	• si • Utilizan el internet	• Si • Mediante el software	• Vishing • phishing	• Mediante software y bases de datos	• mediante el uso de las redes sociales	• mediante redes sociales	• redes sociales • herramientas gigitales

Preguntas /Entrevistado	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
P9	• Si • capacitarse	• Si • Necesitan especializarse	• Si • Necesitan actualizarse	• Si • equipar sus aparatos logísticos	• Si • desconocen de las TIC	• no • si bien es cierto deberían especializarse	• no, carecen de herramientas tecnológicas	• presentan un desconocimiento en la materia	• carecen de información y herramientas	• actualizar información
P10	• SI	• SI	• Si • Diariamente	• SI • Y intercambiar información con otros países	• Si • capacitarse constantemente	• El equipo de la fiscalía debería capacitarse	• proporcionar becas y especializarse	• presentar un presupuesto adecuado	• capacitarse en el extranjero	• orientación al personal de la tic
P11	• No, Pero si me llegan correos maliciosos	• No tengo tarjetas de crédito	• No utilizo • Prefiero pagar en efectivo	• No	• No	• No	• No	• No	• No	• No
P12	• No	• No	• No	• No	• No	• No	• No	• No	• No	• No

ANEXO 5

Tabla 12

Guía de revisión documental bibliográfica-Libro 1

Libro 1		
Título	Delitos Informáticos: Generalidades	
Autor	Juanjo Ramos	año 2022
Objetivo General	----------	
Método	Diseño de la Investigación Explicativo	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		20-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 3,4,5 y 6	
Palabras clave	phishing, correos electrónicos y antivirus	
Referencia Bibliográfica	https://books.google.com.pe/books?id=0kaFEAAAQBAJ&pg=PT2&lpg=PT2&dq=C%C3%B3mo+protegerte+del+phishing:+Evita+que+te+roben+tu+informaci%C3%B3n+y+tu+dinero+Por+Juanjo+Ramos&source=bl&ots=MNbZQi0qrM&sig=ACfU3U3wnRazBQOyr6DQXl4G7XhxtxY_QA&hl=es-419&sa=X&ved=2ahUKEwi295GTzq_8AhXeA7kGHYiSAMIQ6AF6BAgfEAM#v=onepage&q=C%C3%B3mo%20protegerte%20del%20phishing%3A%20Evita%20que%20te%20roben%20tu%20informaci%C3%B3n%20y%20tu%20dinero%20Por%20Juanjo%20Ramos&f=false	
	C1. El phishing está diseñado a engañar a una o más personas para que revelen su información, utilizan las implementaciones de software con el objetivo de secuestrar datos personales.	
	C2. Suelen estar ocultos como mensajes promocionales o utilizan identidades bancarias requiriendo actualización de datos personales y sustraer (usuario y contraseña)	
Conclusiones	C3. El phishing más habitual es por correo electrónico, no están personalizados o dirigidos a una persona en específico, son correos masivos que se dirige cualquier navegador con el objetivo principal de suplantar la identidad	

Nota: *Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV*.

Tabla 13

Guía de revisión documental bibliográfica-Libro 2

Libro 2		
Título	Introducción a la seguridad informática y el análisis de vulnerabilidades	
Autor	Martha Irene Romero Castro Grace Liliana Figueroa Moràn Denisse Soraya Vera Navarrete José Efraín Álava Cruzatty Galo Roberto Parrales Anzúles Christian José Álava Mero Ángel Leonardo Murillo Quimiz Miriam Adriana Castillo Merino	**2018**
Objetivo General	----------	
Método	Diseño de la Investigación Explorativo	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		3-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	13,15,16 y 25	
Palabras clave	virus y seguridad informática	
Referencia Bibliográfica	https://books.google.com.pe/books?hl=es&lr=&id=5Z9yDwAAQBAJ&oi=fnd&pg=PA29&dq=INTRODUCCI%C3%93N+A+LA+SEGURIDAD+INFORM%C3%81TICA+Y+EL+AN%C3%81LISIS+DE+VULNERABILIDADES&ots=ymxPxZf0Vw&sig=lf_WYzzyAJzdrlmiKdhWayIT_SY#v=onepage&q=INTRODUCCI%C3%93N%20A%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20EL%20AN%C3%81LISIS%20DE%20VULNERABILIDADES&f=false	
	C1. Los virus tienen la capacidad de dañar programas relacionados con la red, multiplicándose para ganar posición en partes automatizadas del sistema operativo infectado por la propagación del virus.	
	C2. Los pilares de la seguridad se configuran con la confidencialidad, la integridad y disponibilidad, poseen el nexo de la información para asegurarse que no se pierda o sea corrompible.	
Conclusiones	C3. Los errores humanos o amenazas naturales deben ser controladas antes de poder calcular el riesgo, como también se tiene las amenazas voluntarias que se genera por agente externo internos.	
	C4.las vulnerabilidades se identifican como fallos de diseños que permiten que la amenaza pueda tomar mayor fuerza por sistemas no actualizados o sistemas mal configurados.	

Nota: *Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 14

Guía de revisión documental bibliográfica-Libro 3

Libro 3		
Título	Investigaciones cualitativas en ciencia y tecnología	
Autor	VI Congreso Investigaciones cualitativas en ciencia y tecnología 2017.	**2018**
Objetivo General	El objetivo del presente trabajo es desarrollar el sistema de gestión informática de la DPCGR para administración y control de los recursos tecnológicos y humanos relacionados con las TIC en la institución	
Método	Diseño de la Investigación Explorativo	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		6-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	11,13 y 19	
Palabras clave	sitio web y biblioteca digital	
Referencia Bibliográfica	https://books.google.com.pe/books?id=okdVDwAAQBAJ&lpg=PA1&dq=LIBROS%20DE%20METODOLOGIA%20DE%20INVESTIGACION%20CON%20EDITORIAL%20DEL%202012&pg=PA26#v=onepage&q&f=fal	
	C1.la investigación informática presenta un resultado sostenible se considera factible teniendo en cuenta lo ambiental y tecnológico.	
	C2. La creación de diversos sistemas eficientes a la gestión de información como ordenadores podrá garantizar la dispersión de las barreras cibernéticas.	
Conclusiones	C3. el análisis de la evolución informática se da a medida que la enseñanza y el aprendizaje puedan establecer la calidad respecto a los resultados	
	C4. La tecnología de información constituye a un eje de información mundial, con el respaldo de la enseñanza y aprendizaje para la facilitación del procesamiento de información.	

Nota: *Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 15

Guía de revisión documental bibliográfica-Libro 4

Libro 4		
Título	Segurid ad informática y protección de datos personales	
Autor	José Manuel Ferro Veiga	año 2020
Objetivo General	----------	
Método	Diseño de la Investigación	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		7-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	4,5,6,7,8,9 y 10	
Palabras clave	Ciberdelincuente y IP	
Referencia Bibliográfica	https://books.google.com.pe/books?id=NO7JDwAAQBAJ&pg=PA9&dq=delitos+inform%C3%A1ticos+suplantacion+de+identidad&hl=es-419&sa=X&ved=2ahUKEwjvv-Lkxq_8AhUAHrkGHUBXBUsQ6AF6BAgGEAI#v=onepage&q=delitos%20inform%C3%A1ticos%20suplantacion%20de%20identidad&f=false	
	C1. Las redes de la tecnología se han incrementado debido a la facilidad que posee el ciberdelincuente de pasar inadvertido aprovechando vacíos o agujeros de seguridad que presenta la computadora o laptop del individuo.	
	C2. Se hace difícil al gobierno poder combatir y resguardar la información privada del ciudadano, los ciberdelincuentes utilizan programaciones de software altamente capacitados para vulnerar tu información personal y logra su objetivo de suplantar la identidad; en algunos casos las redes de computación logran extenderse a todo el mundo generando que tu información se encuentre expuesta.	
Conclusiones	C3. Los actos delictivos ocasionados a un hardware son eventos perjudiciales, con la intensión de que un hacker acceda a una Pc o Laptop destruyendo el disco duro y vulnerando la información obteniendo un acceso físico al ordenador.	
	C4. sin embargo, hoy en día se puede rastrear las direcciones de red IP esta acción se está mejorando con el tiempo, lo que hace que sea difícil que el ciberdelincuente pueda mantenerse oculto e invisible en la internet.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 16

Guía de revisión documental bibliográfica-Libro 5

Libro 5			
Título	Derecho y nuevas tecnologías: La influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español		
Autor	Francisco j. Aranda serna	año	2021
Objetivo General	----------		
Método	Diseño de la Investigación		
Instrumento	Ámbito de estudio		Fecha de consulta
Revisión Documental Análisis de datos			24-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	33,49 Y 173		
Palabras clave	phishing, sistema financiero y identidad digital		
Referencia Bibliográfica	https://books.google.com.pe/books?id=pIkxEAAAQBAJ&pg=PT122&dq=delitos+inform%C3%A1ticos+suplantacion+de+identidad&hl=es-419&sa=X&ved=2ahUKEwjq95O9yK_8AhVSJrkGHQIMAxsQ6AF6BAgIEAI#v=onepage&q=delitos%20inform%C3%A1ticos%20suplantacion%20de%20identidad&f=false		
Hay que agregarlo a la discusión	C1. EL robo de la identidad es uno de los delitos que a aumentado con el tiempo, suele tener un solo objetivo que es el robo de información personal para realizar un perjuicio a un usuario.		
	C2. Consiste en realizar una apropiación ilegal de identidad es un fenómeno de manera inmediata en lagunas ocasiones no se manifiesta en un largo tiempo; lo más asociado suelen ser los fraudes o la apropiación de información sensible.		
Conclusiones	C3. El método más utilizado es el phishing que consiste en una estafa por email utilizando la información de una identidad bancaria para la obtención de datos, por otro lado, se tiene a los que ofrecen ofertas de empleo con características atractivas para provecharse de tu contraseña.		
	C4. el método más cruel es el apropiarse la identidad utilizando la introducción de un virus informático o programas capaces de alterar tu información afectando no solo al usuario, sino que también afectan a grandes empresas ocasionado pérdidas económicas.		

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 17

Guía de revisión documental bibliográfica-Libro 6

Libro 6		
Título	Virus Informáticos Máster en Informática	
Autor	Prieto Álvarez, Víctor Manuel Pan Concheiro, Ramón Adrián	año 2021
Objetivo General	----------	
Método	Diseño de la Investigación	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		21-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	10, 13 y 14	
Palabras clave	Virus troyanos y encriptados y antivirus	
Referencia Bibliográfica	https://docplayer.es/980254-Virus-informaticos-master-en-informatica-prieto-alvarez-victor-manuel-pan-concheiro-ramon-adrian.html	
	C1. Los virus se caracterizan por presentar una acción directa respecto al objetivo utilizando un fichero y lograr infectar dentro de un mismo ordenador quedando en algunos casos inservible de tal manera que la información que se tenía no se pueda recuperar.	
	C2. Los virus encriptados buscan camuflarse utilizando técnicas en cada una de sus infecciones buscando captar información confidencial como (contraseñas y números de tarjetas de crédito) dichas técnicas son para no identificarlos por los antivirus.	
Conclusiones	C3. En la actualidad las infecciones se generan por gusano o troyanos trasmitidos a través de internet o páginas web que se va utilizando mediante la búsqueda de información o ordenadores digitales, aprovechando la vulnerabilidad que existe en el ámbito tecnológico (teléfonos iPad y computadoras).	
	C4. Las técnicas que utilizan los ciberdelincuentes para vulnerar la información y violentar los datos personales con el fin es sustraer la información necesaria para realizar la suplantación de identidad y consumar un hecho premeditado.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 18

Guía de revisión documental bibliográfica-Libro 7

Libro 7		
Título	Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú	
Autor	CONAPOC	año 2020
Objetivo General	----------	
Método	Diseño de la Investigación	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		21-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	10, 13 y 14	
Palabras clave	Riesgos amenazas y victimas	
Referencia Bibliográfica	https://cdn.www.gob.pe/uploads/document/file/1616607/Diagn%C3%B3stico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20%20en%20el%20Per%C3%BA.pdf	
	C1. La ciberdelincuencia denominada ciberdelito, conocida como aquellas conductas que burlan el sistema de seguridad mediante clave de acceso, pueden ser sistema de comunicaciones masivos teléfonos celulares y mediante el cual se cometen delitos punibles etc.	
	C2.los riesgos de la criminalidad cibernética se relacionan con los datos y la información personal, la COVID- 19 ayudo a que la tecnología tome mayor notoriedad, los momentos de lucha contra la ciberdelincuencia generan un impacto de brechas asimétricas generando la desigualdad en las TIC, generando una población vulnerable	
Conclusiones	C3. El convenio Budapest presenta un mecanismo que fue utilizado entre los estados miembros del consejo de Europa y los países firmantes, el Perú toma relevancia partir del 2019 suscribiéndose al convenio, siendo el convenio Budapest la puerta a la creación de la ley 30096.	
	C4. Si bien es cierto tenemos la ley N°30096 que hace frente a los delitos informáticos este presenta diversas modalidades como expresiones que son más recurrentes con el tiempo buscando una oportunidad para realizar un hecho criminal vulnerando la información personal.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 19

Guía de revisión documental bibliográfica-Libro 8

Libro 8	
Título	CIBERCRIMEN Y DELITOS INFORMÁTICOS
Autor	MATILDE S. año 2018
Objetivo General	----------
Método	Diseño de la Investigación
Instrumento	Ámbito de estudio / Fecha de consulta
Revisión Documental Análisis de datos	2-noviembre - 2022
Ubicación de la Fuente en el cuerpo del trabajo	33
Palabras clave	Delito cibernético, financiero y tecnología informática
Referencia Bibliográfica	https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf
	C1. La tecnología con el tiempo a generado una nueva forma de adquirir un poder informático, que no ha sido indiferente al derecho, cuando hablamos de tecnología se relaciona con el internet, que modifica con el tiempo la información contribuyendo a l desarrollo social económico y político
	C2. Los delitos informáticos o conductas antijuridicas deben determinarse en un marco penal, teniendo en cuenta el principio de legalidad especificando que no puede haber delito ni pena sin que se presente una ley previa
Conclusiones	C3. El fraude informático en los sistemas financieros se configura mediante el “Phishing” y “pharming” en el primer caso se presentan como identidades bancarias y en el “pharming” consiste en suplantar el nombre de dominio y conducir al ciber navegante a una web falsa.
	C4. De acuerdo a los enfoques presentados como la falta de tipificación en argentina se presentó una Ley 26388 ley de delitos informáticos el cual no es sufriente a los desafíos involucran aspectos jurídicos, políticos y socioculturales.

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 20

Guía de revisión documental bibliográfica-Libro 9

Libro 9		
Título	Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada	
Autor	OFAEC	año 2020
Objetivo General	----------	
Método	Diseño de la Investigación	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		2-noviembre - 2022
Ubicación de la Fuente en el cuerpo del trabajo	19, 34 Y 47	
Palabras clave	Perito digital y Criminalidad informática	
Referencia Bibliográfica	https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf	
	C1. El convenio Budapest hace mención a la legislación penal en relación a los delitos cibernéticos ha garantizado el combatir el fenómeno de la ciberdelincuencia, asimismo es un tratado que nació de los países miembros del consejo de Europa.	
	C2.La DIVINDAT Delitos de Alta Tecnología de la Policía Nacional del Perú registro en el 2020, 12169 casos vinculados a la ley 30096 , ley que nación a raíz del convenio Budapest.	
Conclusiones	C3. La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, fue creada por el debido incremento de la ciberdelincuencia, disponiendo la red de fiscales que serán nexos en cada distrito con la unidad especializada	
	C4. El estudio efectuado a las redes fiscales de la ciberdelincuencia los diversos países como Chile, Argentina, Brasil, Costa Rica utilizan la información electrónica para cometer delitos	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 21

Guía de revisión documental bibliográfica-Libro 10

Libro 10		
Título	CIBERCRIMEN Y DELITOS INFORMÁTICOS	
Autor	Ricardo Antonio Parada; José	año 2018
Objetivo General	----------	
Método	Diseño de la Investigación	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		2-octubre -2022
Ubicación de la Fuente en el cuerpo del trabajo	33,49 y 143	
Palabras clave	protección de datos y era digital	
Referencia Bibliográfica	https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf	
	C1. a raíz que los delitos información fueron tomando mayor relevancia en EE.UU. se logró crear una organización (DARPA)con el fin de contrarrestar ciertos avances puesto que se tuvo grandes perdidas económicas por el gusano Morris, que en la década de los 80 fue un virus muy potente.	
	C2. L a función principal de DARPA es proteger y prevenir de las amenazas informáticas reservando la confidencialidad y autenticidad del usuario, asimismo guardar evidencia suficiente por si el caso llega a manos de la justicia.	
Conclusiones	C3. El cibercrimen para considerarlo en dos áreas específicas se tiene “el derecho” y la “seguridad informática”, en el ámbito del derecho genera una posición sancionatoria cuando se consuma el delito y en términos de seguridad la conjugación y represión del delito.	
	C4 la seguridad informática se enfoca desde una mirada técnica-preventiva tratando de mitigar amenazas (virus gusanos y troyanos) generando fallas en la seguridad e incidentes informáticos de todo tipo.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 22

Guía de revisión documental bibliográfica-Libro 11

Libro 11		
Título	Delitos Informáticos: Generalidades	
Autor	Santiago Acurio Del Pino año	2016
Objetivo General	----------	
Método	Diseño de la Investigación Explorativo	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		20-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 13,25,51,111,112	
Palabras clave	Espionaje, Sabotaje y Delito	
Referencia Bibliográfica	http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/599/Delitos%20Inform%c3%a1ticos.%20generalidades.pdf?sequence=1&isAllowed=y	
	C1. Es necesario reforzar la seguridad de las PC, para proteger de los hacker y piratas informáticos, que podrían paralizar nuestro sistema.	
	C2. Considerar el uso de software que eviten los virus informáticos que podrían vulnerar la computadora y paralizar el uso de las mismas.	
Conclusiones	C3. Finalmente poner a buen recaudo el backag de las nuestras empresas, para evitar el sabotaje de los delincuentes informáticos.	
	C4 Los delitos informáticos, no claramente tipificado en el código penal y la ley N°30096, lo que genera una sanción adecuada.	
	C5. Concluimos que la tecnología es mucha importancia, pero al mismo tiempo es de tiempo cuidado por el incremento de delitos informáticos.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 23

Guía de revisión documental bibliográfica-Libro 12

Libro 12		
Títulos	Delitos informáticos	
Autor	René De Sola Quintero	año 2021
Objetivo General	----------	
Método	Diseño de la Investigación Explorativo	
Instrumento	Ámbito de estudio	Fecha de consulta
Revisión Documental Análisis de datos		20-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 13,25,51,111,112	
Palabras clave	fraude; falsificación y suplantación	
Referencia Bibliográfica	https://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf	
	C1. El delito informático es la acción u omisión realizada por el ser humano que, con el fin de causar un perjuicio a una persona o aun conjunto de personas, aunque no se beneficie de manera directa el coautor genera el beneficio al autor.	
	C2. Por lo que se inferir la red de internet se encuentra vulnerada permite dar soporte al espionaje no autorizado; al narco tráfico para el blanqueo de dinero y a otros delitos las mismas que el internet permite por su débil control.	
Conclusiones	C3. Por otro lado, el tratadista Sarzana pg.3 sostiene que los delitos informáticos son cualquier comportamiento criminal donde se involucra la computadora como material y como objeto principal que utiliza el ciberdelincuente para consumar su hecho ilícito.	
	C4 finalmente los diversos autores consideran que la característica de los ciberdelincuentes (sujetos activos) son personas que no poseen antecedentes delictivos; actúan de forma individual, asimismo poseen una inteligencia brillante con capacidad de concentración y perseverancia.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 24

Guía de revisión documental bibliográfica-Artículo 1

ARTICULO 1			
Título	Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera		
Autor	Juan Pablo Cavada Herrera	año	2020
Objetivo General	----------		
Método	Diseño de la Investigación		
Cualitativo	Explicativo		Fecha de consulta
Instrumento	Ámbito de estudio		
Revisión Documental Análisis de datos	Chile		12-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 13,25,51,111,112		
Palabras clave	Tic y delitos		
Referencia Bibliográfica	https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulaci		
Conclusiones	C1. El convenio Budapest genera indicios que tiene relación con la ciberdelincuencia, por ello el artículo 2 del convenio hace referencia al acceso ilícito el cual obliga a la tipificación como delito el ingreso o acceso deliberado a un sistema informático con intención delictiva.		

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 25

Guía de revisión documental bibliográfica-Artículo

2	ARTICULO 2		
Título	Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales		
Autor	Carmen Leyva Serrano	año	2021
Objetivo General	----------		
Método	Diseño de la Investigación		
Cualitativo	Explicativo		Fecha de consulta
Instrumento	Ámbito de estudio		
Revisión Documental Análisis de datos	Perú		12-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 37,38,39,41,42		
Palabras clave	Valoración de delitos informáticos y bien jurídico protegido		
Referencia Bibliográfica	https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/view/18373/16528		
Conclusiones	C1. La criminología prevista por un delito informático, el cual el delincuente cibernético realiza una conducta delictiva los llamados “Computer Hackers”, con habilidades en el manejo de la informática, con el tiempo los sistemas se desarrollan y el poder de control aumenta en los individuos.		

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 26

Guía de revisión documental bibliográfica-Artículo 3

ARTICULO 3		
Título	DELITOS INFORMATICOS	
Autor	Quintero de Sola, R	año 2021
Objetivo General	----------	
Método	Diseño de la Investigación	
Cualitativo	Explicativo	Fecha de consulta
Instrumento	Ámbito de estudio	
Revisión Documental Análisis de datos	Perú	12-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 7,10,12,18	
Palabras clave	Delito informático, falsificación y espionaje	
Referencia Bibliográfica	https://www.desolapate.com/publicaciones/DELITOS%20INFORMATICOS_RDeSola.pdf	
Conclusiones	C1. Hoy en día el sistema cibernético a perjudicado a varios usuarios que utilizan la tecnología como un medio de pago, considerando este acto como indispensable para continuar con su vida cotidiana, sin embargo existe miedo y desconfianza que la información personal este siendo vulnerada o acechada por los ciberdelincuentes	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 27

Guía de revisión documental bibliográfica-Tesis 1

TESIS 1			
Título	Suplantación de la identidad digital con fines de trata de personas en Facebook”		
Autor	Efraín Aguilar Barrera	año	2019
Objetivo General	----------		
Método	Diseño de la Investigación		
Cualitativo	Explicativo	Fecha de consulta	
Instrumento	Ámbito de estudio		
Revisión Documental		03-septiembre-2022	
Ubicación de la Fuente en el cuerpo del trabajo	11,12,13,24 y 31		
Palabras clave	Identidad digital, suplantación, usurpación y datos		
Referencia Bibliográfica	https://infotec.repositorioinstitucional.mx/jspui/bitstream /1027/363/1/INFOTEC_MDTIC_EAB_26092019.pdf		
Conclusiones	C2. La captación de personas por las distintas redes sociales, se da con la intención de someterlas a la explotación sexual, el robo de la identidad tiene un fin el obtener información financiera y bancaria suplantado la identidad de la víctima con fines de trata de personas.		

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 28

Guía de revisión documental bibliográfica-Tesis 2

TESIS 2		
Título	Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016.	
Autor	Diego Alexander Alarcón Ariza Javier Antonio Barrera Barón	año 2017
Objetivo General	Determinar la relación del uso del internet con los delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, seccional Sogamoso, 2016. de Colombia, seccional Sogamoso, 2016…	
Método	Diseño de la Investigación	
Cualitativo	Explicativo	Fecha de consulta
Instrumento	Ámbito de estudio	
Revisión Documental Análisis de datos		05-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 58,65,68,70,76 y 78	
Palabras clave	Internet, redes sociales y delitos	
Referencia Bibliográfica	https://docplayer.es/88068396-Tesis-uso-de-internet-y-delitos-informaticos-en-los-estudiantes-de-primer-semestre-de-la-universidad-pedagogica-y-tecnologica-de.html	
Conclusiones	C2. El desconocimiento del agraviado de los avances de la ciberdelincuencia entorno a la destreza y la practica reiterada, permite desarrollar habilidades para un alcance de información eficiente y eficaz, los aspectos sociales permiten que se desarrollen con los delitos informáticos, el uso correcto de las redes sociales y el uso legal de la información evidencia que menor será la presencia de delitos en las redes.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 29

Guía de revisión documental bibliográfica-Tesis 3

TESIS 3		
Título	Análisis jurídico de la ley 1273 del 2009 y el surgimiento y expansión del delito de hurto y semejantes por medios informáticos.	
Autor	yenifer yirlesa bechara palacios, Alan yecid mosquera palacios y Edwar estivin Ledezma	año 2020
Objetivo General	----------	
Método	Diseño de la Investigación	
Cualitativo	Explicativo	Fecha de consulta
Instrumento	Ámbito de estudio	
Revisión Documental Análisis de datos		06-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo	15, 17 y 20	
Palabras clave	Hurto, tecnología y código penal colombiano	
Referencia Bibliográfica	http://www.knowledgecap.bigstarcreative.com/bitstream/20.500.12494/19788/3/2020_analisis_delitos_informaticos.pdf	
Conclusiones	El avance de la tecnología ha generado que la sociedad se mantenga alerta de la delincuencia cibernética el cual fluye mediante las redes telemáticas con el objetivo de vulnerar la información personal.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 30

Guía de revisión documental bibliográfica-Tesis 4

TESIS 4			
Título	"Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México.		
Autor	Luis Miguel Carriedo Téllez	año	2022
Objetivo General	----------		
Método	Diseño de la Investigación		
Cualitativo	Explicativo	Fecha de consulta	
Instrumento	Ámbito de estudio		
Revisión Documental Análisis de datos		08-septiembre-2022	
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 21,69 Y 87		
Palabras clave	Censura, delitos informáticos y Internet		
Referencia Bibliográfica	https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/518/1/SOLUCIONESTRATEGICA_LMCT.pdf		
Conclusiones	C2. El convenio Budapest representa la unió de varios países, buscando redimir la tecnología de información y el avance del internet cibernético como una libertad de expresión, la ciberdelincuencia y el uso indebido de la Tic definen a un instrumento ilícito y perjudicial en los medios de comunicación.		

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 31

Guía de revisión documental bibliográfica-Tesis 5

TESIS 5			
Título	El impacto del cibercrimen en delitos de estafa en el Distrito de Lima, 2021.		
Autor	Irma Gisela Huayre Torres	año	2021
Objetivo General	----------		
Método	Diseño de la Investigación		
Cualitativo	Explicativo		Fecha de consulta
Instrumento	Ámbito de estudio		
Revisión Documental Análisis de datos			12-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo	Páginas 13,25,51,111,112		
Palabras clave	Cibercrimen, delito de estafa, delitos informáticos.		
Referencia Bibliográfica	http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1729/TRABAJO%20DE%20INVESTIGACI%c3%93N%20%281%29.pdf?sequence=1&isAllowed=y		
Conclusiones	C2. En la actualidad la vida cada vez más se ha vuelto digitalizada, los usuarios tienen preocupaciones por la seguridad de información personal y patrimonial, Los ciberdelitos no se encuentran limitados en el derecho internacional es por ello que genera una incertidumbre jurisdiccional.		

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 32

Guía de revisión documental bibliográfica-Tesis 6

TESIS 6	
Título	Los delitos informáticos en Perú y la suscripción del convenio de Budapest
Autor	Marleny Yudy Huamán Cruz año 2020
Objetivo General	Explicar la manera en que la suscripción del convenio de Budapest influye en el tratamiento de los delitos informáticos.
Método	Diseño de la Investigación
Cualitativo	Explicativo Fecha de consulta
Instrumento	Ámbito de estudio
Revisión Documental Análisis de datos	Páginas 13,25,51,111,112
Ubicación de la Fuente en el cuerpo del trabajo	
Palabras clave	Virus, clonación de tarjetas y Phishing.
Referencia Bibliográfica	https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/4116/Marleny_Tesis_bachiller_2020.pdf?sequence=1&isAllowed=y
Conclusiones	C2. El convenio Budapest influye en el tratamiento de los delitos informáticos estableciendo normas procesales guiada a salvaguardar las evidencias digitales y datos personales, los delitos informáticos en el Perú han avanzado de manera abismal generando la promulgación de la ley N° 30096 permitiendo tener una legislación comparada delitos informáticos.

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 33

Guía de revisión documental bibliográfica-Tesis 7

TESIS 7			
Título	"Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de lima, periodo 2008 al 2012"		
Autor	Mori Quiroz, Francisco	año	2019
Objetivo General	Conocer la causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de 2012, distrito Judicial de Lima.		
Método	Diseño de la Investigación		
Cuantitativo	Explicativo	Fecha de consulta	
Instrumento	Ámbito de estudio		
Revisión Documental Análisis de datos		12-septiembre-2022	
Ubicación de la Fuente en el cuerpo del trabajo	17,18,19,20		
Palabras clave	Avances tecnológicos, delitos informáticos y interés social.		
Referencia Bibliográfica	https://1library.co/document/q7lrlxoy-delitos-informaticos-proteccion-penal-intimidad-distrito-judicial-periodo.html		
Conclusiones	C2. La tecnología informática ha avanzado generando un procesamiento informático de datos, se caracteriza por que en la mayoría son jóvenes motivados por el desafío técnico generando un cargo de confianza con acceso a materiales privados, la instalación de procesamiento de datos confidenciales puede atentar contra un sistema de tratamiento de información que no logran ser sancionados.		

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 34

Guía de revisión documental bibliográfica-Tesis 8

TESIS 8		
Título	Delitos informáticos en las entidades bancarias - suplantación de identidad	
Autor	Giuliani Marina Monja Esquivel	año 2022
Objetivo General	----------	
Método	Diseño de la Investigación Explorativo	
Cuantitativo	Ámbito de estudio	Fecha de consulta
Instrumento		
Revisión Documental Análisis de datos		07-octubre-2022
Ubicación de la Fuente en el cuerpo del trabajo	9,10,11,12	
Palabras clave	Banco, delitos y	
Referencia Bibliográfica	http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1953/TRABAJO%20DE%20INVES.MONJA%20ESQUIVEL%2c%20GIULIANA%20MARINA.pdf?sequence=1&isAllowed=y	
Conclusiones	C2. La suplantación o robo de la identidad como datos personales, contraseñas y usuarios, se ha generado por un avance tecnológico, teniendo como afectados a los clientes y a los sistemas bancarios, siendo el más común los préstamos, compras online y la clonación de tarjetas de débito, generando la sensibilidad en el cliente.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 35

Guía de revisión documental bibliográfica-Tesis 9

TESIS 9		
Título	Análisis de los medios probatorios idóneos para comprobar los delitos electrónicos en el Distrito Nacional, año 2019.	
Autor	Maritza Santos Lorenzo	año 2020
Objetivo General	Conocer la causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, distrito Judicial de Lima.	
Método	Diseño de la Investigación	
Cuantitativo	Explicativo	Fecha de consulta
Instrumento	Ámbito de estudio	Republica dominicana
Revisión Documental Análisis de datos		12-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo	15,18,19,24	
Palabras clave	Manipulación programas fraudes y herramientas digitales.	
Referencia Bibliográfica	https://bibliotecaunapec.blob.core.windows.net/tesis/TPG_CI_MDP_06_2020_ET210180.pdf	
Conclusiones	C2. La investigación del campo cibernético permite extraer datos personales e información digitalizada a través de herramientas digitales utilizando técnicas de recolección permitiendo describir y comprobar los delitos electrónicos, es necesario concientizar la protección de datos personales en las redes sociales	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 36

Guía de revisión documental bibliográfica-Tesis 10

TESIS 10			
Título	SUPLANTACION DE IDENTIDAD: Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino		
Autor	Montaperto, Javier Eduardo.	año	2018
Objetivo General	El objetivo consiste en realizar un análisis sobre la falta de regulación en el ordenamiento jurídico argentino de la suplantación de la identidad de la persona aún luego de la reforma del Código Penal mediante ley Nº 26.388 de delitos informáticos.		
Método	Diseño de la Investigación		
Cuantitativo	Explicativo	Fecha de consulta	
Instrumento	Ámbito de estudio		
Revisión Documental Análisis de datos		10-septiembre-2022	
Ubicación de la Fuente en el cuerpo del trabajo	15,18,19,24		
Palabras clave	Suplantación de identidad de la persona – principio penal de legalidad		
Referencia Bibliográfica	https://www.pensamientopenal.com.ar/doctrina/90107-suplantacion-identidad-analisis-sobre-su-falta-regulacion-ordenamiento-juridico		
Conclusiones	C2. La suplantación de identidad se genera mediante un ataque informático utilizando la ingeniería social, filtrando con engaño información confidencial de la víctima, provocando perjuicio patrimonial como también el derecho a la propiedad, en el ámbito extrapatrimonial, vulnerando del buen nombre imagen y prestigio.		

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 37

Guía de revisión documental bibliográfica-Tesis 11

TESIS 11		
Título	Los delitos informáticos y los vacíos legales que afectan a los ciudadanos	
Autor	Chiluisa Mullo Dany	año 202
Objetivo General	Elaborar un ensayo critico jurídico en evidencia de los vacíos legales existentes en el ordenamiento jurídico ecuatoriano y que tienen relación con los delitos informáticos que actualmente afectan a los ciudadanos.	
Método	Diseño de la Investigación	
Cuantitativo	Explicativo	Fecha de consulta
Instrumento	Ámbito de estudio	
Revisión Documental Análisis de datos		10-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo		
Palabras clave	Anónimo y tutela efectiva	
Referencia Bibliográfica	http://repositorio.ucsg.edu.ec/bitstream/3317/16501/1/T-UCSG-PRE-JUR-DER-MD-334.pdf	
Conclusiones	C2. La delincuencia cibernética a transgredido fronteras dejando sin protección a miles de personas que hoy en día utilizan la tecnología con fuente de ingreso, si lo vemos desde el ámbito legal requiere ser más rigurosa con lo ciberdelincuentes, puesto que con el tiempo el avance de la tecnología se genera nuevas formas de delinquir.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 38

Guía de revisión documental bibliográfica-Tesis 12

TESIS 12		
Título	"ANÁLISIS DEL DELITO DE HURTO DE IDENTIDAD VIRTUAL: FRENTE A LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS"	
Autor	BRENDA PATRICIA INFANTE año 2019	
Objetivo General	¿La falta de una adecuada seguridad de los sistemas informáticos, facilita el hurto de la identidad virtual?	
Método	Diseño de la Investigación	
Cuantitativo	Explicativo	Fecha de consulta
Instrumento	Ámbito de estudio	
Revisión Documental Análisis de datos		10-septiembre-2022
Ubicación de la Fuente en el cuerpo del trabajo		
Palabras clave	Hurto y identidad	
Referencia Bibliográfica	https://repositorio.unp.edu.pe/bitstream/handle/20.500.12676/2524/DECP-INF-GUE-2019.pdf?sequence=1&isAllowed=y	
Conclusiones	C2.. El hurto de la información personal se manifiesta como una conducta indebida, será sancionada toda vez que se encuentre las pruebas que se utilizaron para su beneficio con el fin de vulnerar la información de la víctima de manera ilícita.	

Nota*: Adaptado de Chávez Suárez Giancarlo Renán, material de clase, UCV.*

Tabla 39

Matriz de codificación de resultados de libros

N°	Título	Autor/es	Año de Publicación	Conclusiones	Codificación
1	Delitos Informáticos: Generalidades	Juanjo Ramos	2022	C1. El phishing está diseñado a engañar a una o más personas para que revelen su información, utilizan las implementaciones de software con el objetivo de secuestrar datos personales. C2. Suelen estar ocultos como mensajes promocionales o utilizan identidades bancarias requiriendo actualización de datos personales y sustraer (usuario y contraseña). C3. El phishing mas habitual es por correo electrónico, no están personalizados o dirigidos a una persona en específico, son correos masivos que se dirige cualquier navegador con el objetivo principal de suplantar la identidad.	L1

2	introducción a la seguridad informática y el análisis de vulnerabilidades	Martha Irene Romero Castro, Grace Liliana Figueroa Moràn ,Denisse Soraya Vera Navarrete, José Efraín Álava Cruzatty ,Galo Roberto Parrales Anzúles ,Christian José Álava Mero, Ángel Leonardo Murillo Quimiz, Miriam Adriana Castillo Merino.	2018	C1. Los virus tienen la capacidad de dañar programas relacionados con la red, multiplicándose para ganar posición en partes automatizadas del sistema operativo infectado por la propagación del virus. C2. Los pilares de la seguridad se configuran con la confidencialidad, la integridad y disponibilidad, poseen el nexo de la información para asegurarse que no se pierda o sea corrompible. C3. Los errores humanos o amenazas naturales deben ser controladas antes de poder calcular el riesgo, como también se tiene las amenazas voluntarias que se genera por agente externo internos. C4.las vulnerabilidades se identifican como fallos de diseños que permiten que la amenaza pueda tomar mayor fuerza por sistemas no actualizados o sistemas mal configurados.	L2

3	Investigaciones cualitativas en ciencia y tecnología.	VI Congreso Investigaciones cualitativas en ciencia y tecnología 2017	2018	C1.la investigación informática presenta un resultado sostenible se considera factible teniendo en cuenta lo ambiental y tecnológico. C2. La creación de diversos sistemas eficientes a la gestión de información como ordenadores podrá garantizar la dispersión de las barreras cibernéticas. C3. el análisis de la evolución informática se da a medida que la enseñanza y el aprendizaje puedan establecer la calidad respecto a los resultados C4. La tecnología de información constituye a un eje de información mundial, con el respaldo de la enseñanza y aprendizaje para la facilitación del procesamiento de información.	L3

4	Seguridad informática y protección de datos personales	José Manuel Ferro Veiga	2020	C1. Las redes de la tecnología se han incrementado debido a la facilidad que posee el ciberdelincuente de pasar inadvertido aprovechando vacíos o agujeros de seguridad que presenta la computadora o laptop del individuo. C2. Se hace difícil al gobierno poder combatir y resguardar la información privada del ciudadano, los ciberdelincuentes utilizan programaciones de software altamente capacitados para vulnerar tu información personal y logra su objetivo de suplantar la identidad; en algunos casos las redes de computación logran extenderse a todo el mundo generando que tu información se encuentre expuesta. C3. Los actos delictivos ocasionados a un hardware son eventos perjudiciales, con la intensión de que un hacker acceda a una Pc o Laptop destruyendo el disco duro y vulnerando la información obteniendo un acceso físico al ordenador . C4. sin embargo, hoy en día se puede rastrear las direcciones de red IP esta acción se esta mejorando con el tiempo, lo que hace que sea difícil que el ciberdelincuente pueda mantenerse oculto e invisible en la internet.	L4

5	Derecho y nuevas tecnologías: La influencia de internet en la regulación de los derechos de la personalidad y los retos digitales del ordenamiento jurídico español.	Francisco j. Aranda serna	2021	C1. EL robo de la identidad es uno de los delitos que a aumentado con el tiempo, suele tener un solo objetivo que es el robo de información personal para realizar un perjuicio a un usuario. C2. Consiste en realizar una apropiación ilegal de identidad es un fenómeno de manera inmediata en lagunas ocasiones no se manifiesta en un largo tiempo; los más asociado suelen ser los fraudes o la apropiación de información sensible. C3. El método más utilizado es el phishing que consiste en una estafa por email utilizando la información de una identidad bancaria para la obtención de datos, por otro lado se tiene a los que ofrecen ofertas de empleo con características atractivas para provecharse de tu contraseña. C4. el método más cruel es el apropiarse la identidad utilizando la introducción de un virus informático o programas capaces de alterar tu información afectando no solo al usuario sino que también afectan a grandes empresas ocasionado pérdidas económicas.	L5

6	Virus Informáticos Máster en Informática	Prieto Álvarez, Víctor Manuel Y Pan Concheiro, Ramón Adrián	2021	C1. Los virus se caracterizan por presentar una acción directa respecto al objetivo utilizando un fichero y lograr infectar dentro de un mismo ordenador quedando en algunos casos inservible de tal manera que la información que se tenia no se pueda recuperar . C2.Los virus encriptados buscan camuflarse utilizando técnicas en cada una de sus infecciones buscando captar información confidencial como (contraseñas y números de tarjetas de crédito)dichas técnicas son para no identificarlos por los antivirus. C3. En la actualidad las infecciones se generan por gusano o troyanos trasmitidos a través de internet o páginas web que se va utilizando mediante la búsqueda de información o ordenadores digitales, aprovechando la vulnerabilidad que existe en el ámbito tecnológico (teléfonos ipad y computadoras). C4. Las técnicas que utilizan los ciberdelincuentes para vulnerar la información y violentar los datos personales con el fin es sustraer la información necesaria para realizar la suplantación de identidad y consumar un hecho premeditado .	L6

Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú	7	CONAPOC	2020	C1. La ciberdelincuencia denominada ciberdelito, conocida como aquellas conductas que burlan el sistema de seguridad mediante clave de acceso, pueden ser sistema de comunicaciones masivos teléfonos celulares y mediante el cual se cometen delitos punibles etc. C2.los riesgos de la criminalidad cibernética se relacionan con los datos y la información personal, la COVID- 19 ayudo a que la tecnología tome mayor notoriedad, los momentos de lucha contra la ciberdelincuencia generan un impacto de brechas asimétricas generando la desigualdad en las TIC, generando una población vulnerable C3. El convenio Budapest presenta un mecanismos que fue utilizado entre los estados miembros del consejo de Europa y los países firmantes , el Perú toma relevancia partir del 2019 suscribiéndose al convenio , siendo el convenio Budapest la puerta a la creación de la ley 30096. C4. Si bien es cierto tenemos la ley N°30096 que hace frente a los delitos informáticos este presenta diversas modalidades como expresiones que son más recurrentes con el tiempo buscando una oportunidad para realizar un hecho criminal vulnerando la información personal .	L7

8	cibercrimen y delitos informáticos	Matilde s. Martínez	2018	

C1.La tecnología con el tiempo a generado una nueva forma de adquirir un poder informático, que no ha sido indiferente al derecho, cuando hablamos de tecnología se relaciona con el internet, que modifica con el tiempo la información contribuyendo a l desarrollo social económico y político
C2. Los delitos informáticos o conductas antijuridicas deben determinarse en un marco penal, teniendo en cuenta el principio de legalidad especificando que no puede haber delito ni pena sin que se presente una ley previa
C3. El fraude informático en los sistemas financieros se configura mediante el “Phishing” y “pharming” en el primer caso se presentan como identidades bancarias y en el “pharming” consiste en suplantar el nombre de dominio y conducir al cibernavegante a una web falsa .
C4.De acuerdo a los enfoques presentados como la falta de tipificación en argentina se presentó una Ley 26388 ley de delitos informáticos el cual no es sufriente a los desafíos involucran aspectos jurídicos , políticos y socioculturales.

L8

9	Ciberdelincuencia en el Perú: pautas para una investigación fiscal especializada	**OFAEC**	2020	C1.El convenio Budapest hace mención a la legislación penal en relación a los delitos cibernéticos ha garantizado el combatir el fenómeno de la ciberdelincuencia, asimismo es un tratado que nació de los países miembros del consejo de Europa. C2.La DIVINDAT Delitos de Alta Tecnología de la Policía Nacional del Perú registro en el 2020, 12169 casos vinculados a la ley 30096. C3. La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, fue creada por el debido incremento de la ciberdelincuencia, disponiendo la red de fiscales que serán nexos en cada distrito con la unidad especializada C4. El estudio efectuado a las redes fiscales de la ciberdelincuencia los diversos países como Chile, Argentina, Brasil, Costa Rica utilizan la información electrónica para cometer delitos.	L9

10	Cibercrimen y delitos informáticos	Ricardo Antonio Parada y José Daniel Errecaborde.	2018	C1. a raíz que los delitos información fueron tomando mayor relevancia en EE.UU. se logró crear una organización (DARPA)con el fin de contrarrestar ciertos avances puesto que se tuvo grandes perdidas económicas por el gusano Morris, que en la década de los 80 fue un virus muy potente. C2. L a función principal de DARPA es proteger y prevenir de las amenazas informáticas reservando la confidencialidad y autenticidad del usuario, asimismo guardar evidencia suficiente por si el caso llega a manos de la justicia. C3. El cibercrimen para considerarlo en dos áreas específicas se tiene “el derecho” y la “seguridad informática”, en el ámbito del derecho genera una posición sancionatoria cuando se consuma el delito y en términos de seguridad la conjugación y represión del delito. C4 la seguridad informática se enfoca desde una mirada técnica-preventiva tratando de mitigar amenazas (virus gusanos y troyanos) generando fallas en la seguridad e incidentes informáticos de todo tipo.	L10

11	Delitos Informáticos: Generalidades	Santiago Acurio Del Pino	2005	C1. Es necesario reforzar la seguridad de las PC, para proteger de los hacker y piratas informáticos, que podrían paralizar el sistema. C2. Considerar el uso de software que eviten los virus informáticos que podrían vulnerar la computadora y paralizar el uso de las mismas C3. Finalmente poner a buen recaudo el backag de las nuestras empresas, para evitar el sabotaje de los delincuentes informáticos. C4.Los delitos informáticos, no están claramente tipificado en el código penal y la ley N°30096, no que genera una sanción adecuada. C5. Concluimos que la tecnología es mucha importancia, pero al mismo tiempo es de tiempo cuidado por el incremento de delitos informáticos.	L11

12	Delitos informáticos	René De Sola Quintero	2021	C1. El delito informático es la acción u omisión realizada por el ser humano que con el fin de causar un perjuicio a una persona o aun conjunto de personas, aunque no se beneficie de manera directa el coautor genera el beneficio al autor. C2. Por lo que se inferir la red de inernet se encuentra vulneraday permite dar soporte al espionaje no autorizado ; al narco trafico para el blanqueo de dinero y a otros delitos las mismas que el internet permite por su débil control . C3. Por otro lado el tratadista Sarzana pg.3 sostiene que los delitos informáticos son cualquier comportamiento criminal donde se involucra la computadora como material y como objeto principal que utiliza el ciberdelincuente para consumar su hecho ilícito. C4 finalmente los diversos autores consideran que la característica de los ciberdelincuentes (sujetos activos) son personas que no poseen antecedentes delictivos; actúan de forma individual, asimismo poseen una inteligencia brillante con capacidad de concentración y perseverancia. .	L12

Tabla 40

Matriz de codificación del resultado del artículo

N°	Título	Autor/es	Año de Publicación	Conclusiones	Codificación
1	Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera	Juan Pablo Cavada Herrera	2020	C1. El convenio Budapest genera indicios que tiene relación con la ciberdelincuencia, por ello el artículo 2 del convenio hace referencia al acceso ilícito el cual obliga a la tipificación como delito el ingreso o acceso deliberado a un sistema informático con intención delictiva.	A1
2	Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales	Carmen Leyva Serrano	2021	C2. La criminología prevista por un delito informático, el cual el delincuente cibernético realiza una conducta delictiva los llamados “Computer Hackers”, con habilidades en el manejo de la informática, con el tiempo los sistemas se desarrollan y el poder de control aumenta en los individuos.	A2

3	DELITOS INFORMATICOS	Quintero de Sola, R	2021	C1. Hoy en día el sistema cibernético a perjudicado a varios usuarios que utilizan la tecnología y sus aplicaciones como un medio de pago, considerando este acto como indispensable para continuar con su vida cotidiana, sin embargo existe miedo y desconfianza que la información personal este siendo vulnerada o acechada por los ciberdelincuentes	A3

Tabla 41

Matriz de codificación de resultados de tesis

N°	Título	Autor/es	Año de Publicación	Conclusiones	Codificación
1	"Suplantación de la identidad digital con fines de trata de personas en Facebook"	Efraín Aguilar Barrera	2019	C1. La captación de personas por las distintas redes sociales, se da con la intención de someterlas a la explotación sexual, el robo de la identidad tiene un fin el obtener información financiera y bancaria suplantado la identidad de la víctima con fines de trata de personas.	T1
2	Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016.	Diego Alexander Alarcón Ariza Y Javier Antonio Barrera Barón	2021	C1. La criminología prevista por un delito informático, el cual el delincuente cibernético realiza una conducta delictiva los llamados "Computer Hackers", con habilidades en el manejo de la informática, con el tiempo los sistemas se desarrollan y el poder de control aumenta en los individuos.	T2

3	El delito de suplantación de identidad y los medios informáticos en el sector financiero de Lima, 2019	Aldecoa Jiménez, Milagros del Rosario	2020	C2. El uso de las diversas técnicas informáticas ha generado la obtención de la información directa de los datos personales del agraviado, por el desmesurado uso de mecanismos tecnológicos que favorece a un delito de suplantación de identidad.	T3
4	“Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México.	Luis Miguel Carriedo Téllez	202	C2. El convenio Budapest representa la unió de varios países, buscando redimir la tecnología de información y el avance del internet cibernético como una libertad de expresión, la ciberdelincuencia y el uso indebido de la Tic definen a un instrumento ilícito y perjudicial en los medios de comunicación.	T4

5	El impacto del cibercrimen en delitos de estafa en el Distrito de Lima, 2021.	Irma Gisela Huayre Torres	2021	C2. En la actualidad la vida cada vez más se ha vuelto digitalizada, los usuarios tienen preocupaciones por la seguridad de información personal y patrimonial, Los ciberdelitos no se encuentran limitados en el derecho internacional es por ello que genera una incertidumbre jurisdiccional.	T5
6	Los delitos informáticos en Perú y la suscripción del convenio de Budapest	Prieto Álvarez, Víctor Manuel Y Pan Concheiro, Ramón Adrián	2020	C2. El convenio Budapest influye en el tratamiento de los delitos informáticos estableciendo normas procesales guiada a salvaguardar las evidencias digitales y datos personales, los delitos informáticos en el Perú han avanzado de manera abismal generando la promulgación de la ley N° 30096 permitiendo tener una legislación comparada delitos informáticos.	T6

7	"Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de lima, periodo 2008 al 2012"	Mori Quiroz, Francisco	2019	C2. La tecnología informática ha avanzado generando un procesamiento informático de datos, se caracteriza por que en la mayoría son jóvenes motivados por el desafío técnico generando un cargo de confianza con acceso a materiales privados, la instalación de procesamiento de datos confidenciales puede atentar contra un sistema de tratamiento de información que no logran ser sancionados.	T7
8	Delitos informáticos en las entidades bancarias -suplantación de identidad	Giuliani Marina Monja Esquivel	2022	C2. La suplantación o robo de la identidad como datos personales, contraseñas y usuarios, se ha generado por un avance tecnológico, teniendo como afectados a los clientes y a los sistemas bancarios, siendo el más común los préstamos, compras online y la clonación de tarjetas de débito, generando la sensibilidad en el cliente.	T8

9	Análisis de los medios probatorios idóneos para comprobar los delitos electrónicos en el Distrito Nacional, año 2019.	Maritza Santos Lorenzo	2020	C2. La investigación del campo cibernético permite extraer datos personales e información digitalizada a través de herramientas digitales utilizando técnicas de recolección permitiendo describir y comprobar los delitos electrónicos, es necesario concientizar la protección de datos personales en las redes sociales.	T9
10	SUPLANTACION DE IDENTIDAD: Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino	Montaperto, Javier Eduardo	2018	C2. La suplantación de identidad se genera mediante un ataque informático utilizando la ingeniería social, filtrando con engaño información confidencial de la víctima, provocando perjuicio patrimonial como también el derecho a la propiedad, en el ámbito extrapatrimonial, vulnerando del buen nombre imagen y prestigio.	T10

11	“Los delitos informáticos y los vacíos legales que afectan a los ciudadanos	Chiluisa Mullo Dany Oswaldo.	2021	C2. La delincuencia cibernética ha transgredido fronteras dejando sin protección a miles de personas que hoy en día utilizan la tecnología con fuente de ingreso, si lo vemos desde el ámbito legal requiere ser más rigurosa con los ciberdelincuentes, puesto que con el tiempo el avance de la tecnología se genera nuevas formas de delinquir.	T11
12	“ “Análisis del delito de hurto de identidad virtual: frente a la seguridad de los sistemas informáticos”	Brenda patricia infante Guevara	2019	C2. El hurto de la información personal se manifiesta como una conducta indebida, será sancionada toda vez que se encuentre las pruebas que se utilizaron para su beneficio con el fin de vulnerar la información de la víctima de manera ilícita del buen nombre imagen y prestigio.	T12

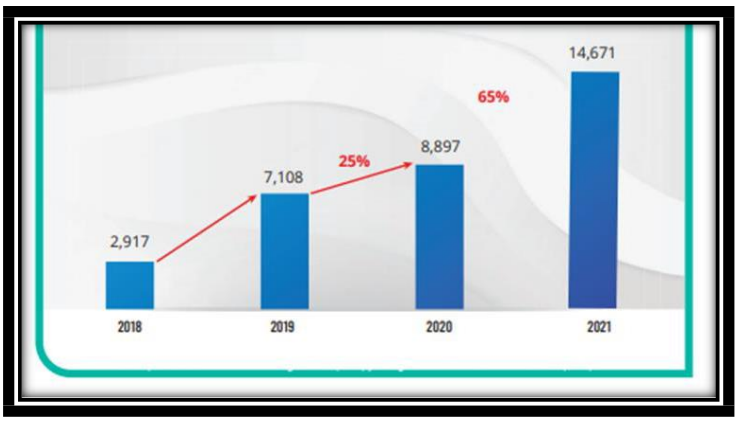
Anexo 6

	Expertos								
ítems	**1**	**2**	**3**	**4**	**5**	**6**	**Suma total de acuerdos (S)**	**V Aiken**	**Descripción**
1	3	2	3	2	3	3	16	0.89	Aceptable
2	3	2	3	2	3	2	15	0.83	Aceptable
3	3	2	3	2	1	3	14	0.78	Débil
4	3	2	3	2	2	3	15	0.83	Aceptable
5	3	2	3	2	3	3	16	0.89	Aceptable
6	3	2	3	2	2	3	15	0.83	Aceptable
7	3	3	3	1	3	3	16	0.89	Aceptable
8	3	3	3	3	3	3	18	1	Fuerte
9	3	2	3	3	1	3	15	0.83	Aceptable
10	3	3	3	2	3	3	17	0.94	Fuerte
11	3	3	3	3	2	3	17	0.94	Fuerte
12	3	3	3	3	3	3	18	1	Fuerte

Adaptado de “Validez de instrumentos de investigación”, por Solís, C., 2020, Material académico del curso Estadística aplicada a la investigación, Universidad Continental, Huancayo.

Figura 12

Variación porcentual de denuncias por delitos informáticos registrados en la PNP 2018-2021.

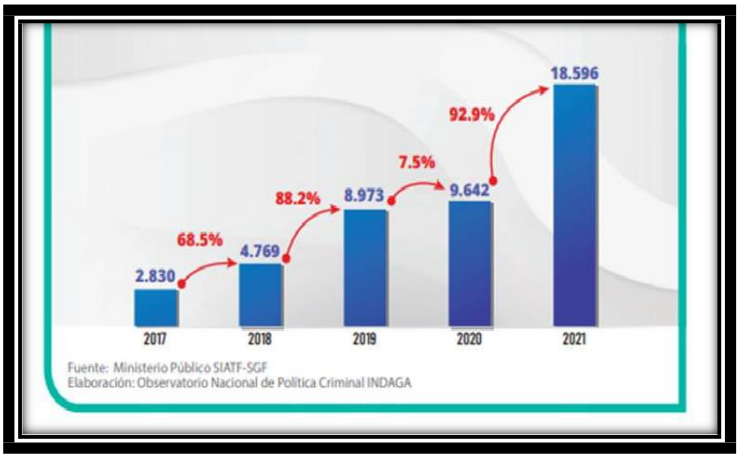


Fuente: Flores, Rodríguez, Urbizagastegui, Guerra y Retuerto (2022) *Ciberdelincuencia reporte de información estadística y recomendaciones para la prevención* Ministerio de justicia y derechos humanos, *Perú https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf?v=1661790352*

Como se puede evidenciar en la figura 12, se presenta un índice de crecimiento de denuncia por delitos informáticos en la PNP, respecto del 2021 y el 2020 el índice de crecimiento es 65% consecuentemente el 2020 y el 2019 se presenta un índice de crecimiento de 25% si hacemos una comparación del 2019 y el 2021 se puede evidencia que la denuncias por delitos informáticos han tomado relevancia un 40%.

Figura 13

Denuncias en el Ministerio Publico a Nivel Nacional 2017-2021.



Fuente: Flores, Rodríguez, Urbizagastegui, Guerra y Retuerto (2022) *Ciberdelincuencia reporte de información estadística y recomendaciones para la prevención* Ministerio de justicia y derechos humanos, *Perú https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf?v=1661790352*

Asimismo, se puede evidenciar en la figura 13, se presenta un índice de crecimiento de denuncia por delitos informáticos en él MP, respecto del 2021 y el 2020 el índice de crecimiento es 92.9% consecuentemente el 2020 y el 2019 se presenta un índice de crecimiento de 75% si hacemos una comparación del 2019 y el 2021 se puede evidencia que la denuncias por delitos informáticos han tomado relevancia un 17.9%.

Figura 14

Denuncias según la ley de delitos informáticos, modificado por ley 30171, por modalidad 2019,2020 y 2021.

Modalidad	2019	2020	2021
Fraude informático *	5,878	6,946	10,924
Suplantación de identidad *	462	935	2,666
Abuso de mecanismos y dispositivos informáticos	258	572	538
Atentado a la integridad de datos informáticos *	255	164	226
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos *	72	82	98
Atentado a la integridad de sistemas informáticos *	65	72	86
Interceptación de datos informáticos *	83	75	69
Acceso ilícito *	35	51	64
Total	**7,108**	**8,897**	**14,671**

Fuente: Flores, Rodríguez, Urbizagastegui, Guerra y Retuerto (2022) *Ciberdelincuencia reporte de información estadística y recomendaciones para la prevención* Ministerio de justicia y derechos humanos, *Perú https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf?v=1661790352*

Por otro lado, en la Figura 14, podemos evidenciar que los delitos informáticos mas asiduos en el Perú son el fraude informático y la suplantación de identidad que ha tomado mayor relevancia en los últimos años.

Figura 15

Denuncias según la ley de delitos informáticos, modificado por ley 30171, por modalidad 2021.

Modalidad	2021	%
Fraude informático *	10,924	74.5%
Suplantación de identidad *	2,666	18.2%
Abuso de mecanismos y dispositivos informáticos	538	3.7%
Atentado a la integridad de datos informáticos *	226	1.5%
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos *	98	0.7%
Atentado a la integridad de sistemas informáticos *	86	0.6%
Interceptación de datos informáticos *	69	0.5%
Acceso ilícito *	64	0.4%
Total	**14,671**	**100%**

Fuente: Flores, Rodríguez, Urbizagastegui, Guerra y Retuerto (2022) *Ciberdelincuencia reporte de información estadística y recomendaciones para la prevención* Ministerio de justicia y derechos humanos, *Perú https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf?v=1661790352*

Para finalizar podemos evidenciar la figura 15, donde se presenta uno de los delitos más asiduos la suplantación de identidad con un porcentaje de 18.2% solo para el año 2021 quiere decir que ha tomado relevancia en los últimos años.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, CHAVEZ SUAREZ GIANCARLO RENAN, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Análisis jurídico de la ineficacia de la Ley N°30096 en el delito de suplantación de identidad por medios informáticos", cuyos autores son QUISPE AYALA VICTOR FAUSTINO, QUISPE SAIRE LAURA SOFIA, constato que la investigación tiene un índice de similitud de 26.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 12 de Febrero del 2023

Apellidos y Nombres del Asesor:	**Firma**
CHAVEZ SUAREZ GIANCARLO RENAN **DNI:** 46877136 **ORCID:** 0000-0001-8053-6136	Firmado electrónicamente por: GRCHAVEZS el 12-02-2023 12:23:16

Código documento Trilce: TRI - 0532695

INVESTIGA UCV